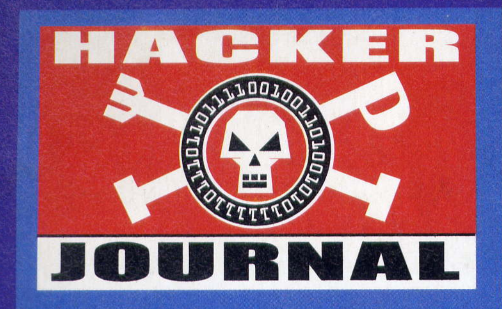


TODO LO QUE NADIE HA OSADO DECIRTE ANTES
HACKER JOURNAL
n. 11
www.hacker-journal.com
BIMESTRAL AÑO 3 - 2005
OSI: CHÁCHARA ENTRE MÁQUINAS
RFID
EL CHIP DE
SEGUIMIENTO
HACKEAR
UNA LINUX LIVE
2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS
DE LA TEORÍA al VoIP:
HABLAR POR IP
P2P:
REDES Y
PROGRAMAS
QUE LO USAN
SECRETOS POR DESCUBRIR
Los retos
QUE PROPONE LA RSA
4ever
00011
8 413042 435235



Año 3 - N. 11 - 2005

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Amadeu Brugués, Eric Sala, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Eric Sala, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Difusión: Paul-Luc PEREZ

Distribución
SGEL - Avda Valdelaparra 29
Polígono Industrial De Alcobendas
Madrid - Spain

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

HABLAR LIBREMENTE

La libertad de palabra es un derecho tan antiguo como la humanidad. Era lógico que tarde o temprano Internet, uno de los modernos espejos de las pasiones y anhelos humanos, reflejara este hecho en sus contenidos. Y está llegando con fuerza a través de las tecnologías de Voz por IP (VoIP). A partir de algo tan elemental como que la voz humana se puede digitalizar y, por lo tanto, viajar por la Red, es lógico que aparezcan soluciones que lo aprovechen para tender puentes entre los usuarios.

Programas como Skipe están empezando a conseguir la masa crítica suficiente para llamar la atención. Con uno de estos programas se puede establecer una conferencia con cualquier otro usuario que disponga del mismo programa. Si contamos con tarifa plana en la conexión a Internet, no tendremos que pagar ni un céntimo para hablar todo el día con los lugares más recónditos del planeta. ¿Los frenos? Muchos hogares no cuentan aún con conexión a Internet. Como ocurrió en su día con el teléfono, si al otro lado no hay nadie es el invento más inútil de la historia. Decía el Perich, un agudo humorista ya desaparecido, que el verdadero genio no fue quien descubrió el primer teléfono, sino el que descubrió el segundo... Con la Voz por IP ocurre algo parecido. Sin embargo, el aumento de usuarios es continuo, por lo que la situación está, de hecho, dando ya el vuelco crítico.

Los principales problemas a los que se enfrenta a largo plazo la Voz por IP son inherentes a Internet. En primer lugar, el fugaz paso de las modas. Magníficas herramientas como los foros de discusión, las news, los portales, el correo instantáneo, los blogs... suelen tener un ascenso meteórico para caer acto seguido a los pies de la siguiente moda de la Red. ¿Por qué apostar fuerte por la VoIP si no sabemos seguro si se va a imponer? Y aún en el caso de que se imponga, ¿qué estándar, qué protocolo será el que se lleve el gato al agua? La mejor propuesta es: instala tu programa de VoIP y, como el filósofo, siéntate a esperar. ¡O bien ponte de acuerdo con tus amigos!

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS



NEWBIE



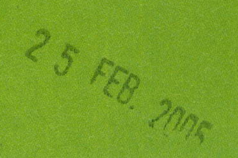
MID HACKING

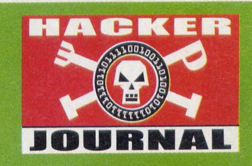


HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO



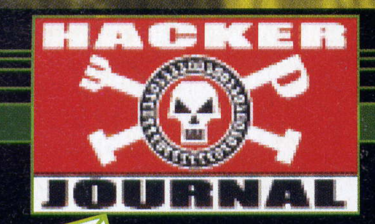


SITIO WEB

Como en cada número de Hacker Journal, os recordamos que tenéis a vuestra disposición el sitio web de la revista, www.hacker-journal.com, para seguir leyendo y aprendiendo sobre el Hacking. Recordad también que disponéis de los foros donde podéis exponer dudas y preguntas, observaciones, etcétera. Todos los visitantes del sitio web colaborarán en hallar respuesta a todas las preguntas. ¡Entre todos lo conseguiremos!

Visita nuestro sitio web:
www.hacker-journal.com

CODIGO DE LA SECRET ZONE
user: secreto11
password: 1decimo







redaccion@hacker-journal.com

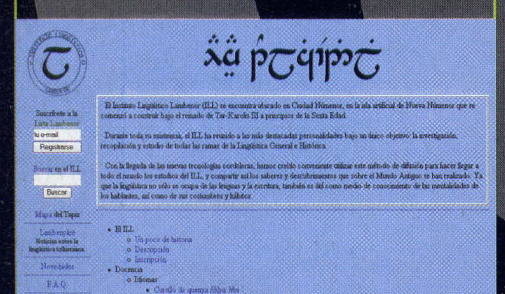
SOBRE EL CYBERENIGMA

Hola me llamo Lara y soy de Gijón y soy una fiel seguidora del Hacker journal desde el primer numero y de vez en cuando del Hackers magazine. En este último numero le he echado un vistazo al ciberenigma que proponíais y he descubierto despues de buscar que las frases pertenecen a la lingüitica tolkieniana, el primer texto pertenece a una lengua conocida por Cirth o Runas y las otras al lenguaje Quenya y/o simbologia Tengwar he encontrado la solucion en la pagina web del instituto lingüístico lambenor y la web es: http://lambenor.free.fr donde se pueden encontrar los alfabetos completos y el modo de crear y traducir frases.

Gracias. Saludos

LARA

Enhorabuena, Lara, por tu magnífica búsqueda. Efectivamente, el Instituto Lingüístico Lambenor es un lugar de referencia para aclarar el cyberenigma propuesto, así como para conocer más sobre las lenguas del mundo de Tolkien.

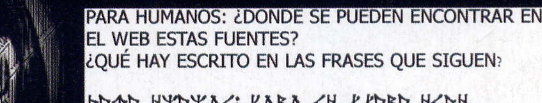


MÁS CYBERENIGMA

wenas!
el otro dia, de viaje en tren, me dio por comerme la cabeza con vuestra ultima pagina de hacker-journal.
Preguntais donde se pueden encontrar y qué dicen... pues bien, no me gustó mucho el Señor de los anillos, pero me di un paseo por inforol.com y alli hay fuentes de esas... al menos eso dice Google, pues no me paré a entrar para descargarme las fuentes. ya en el tren conseguí sacar que decían los dos primeros parrafos, sin contar con el que está en el alfabeto castellano, claro.
El primero, el que es para enanos, dice: para enanos: como se llama este alfabeto? que raza lo usa en el señor de los anillos?
bueno, supongo que la respuesta a la segunda sera Enanos, no lo sé, no soy un friki del señor de los anillos. y el alfabeto, pos no se como se llama, bastante tuve con saber qué decía sin tener las fuentes ¿no? aunque tampoco fue difícil, la verdad.
el segundo parrafo es tanto de lo mismo, aunque creo que faltan letras ¿no?
bueno, este dice: para elfos: como se llama este alfabeto? que raza lo usa en el señor de los anillos? conoces un sitio donde aprender a escribir con este alfabeto?
no se si quereis que contestemos tambien a estas preguntas, pero supongo que cualquier friki podria contestar de p*** madre.
Cuando me metí con el tercer párrafo ya habia llegado el tren a Madrid, así que lo dejé... y ahí está, sin tocar... algún día me pondré, pero ahora mismo casi que no tengo ganas...
Bueno, es lo unico que tengo, supongo que sin tener las fuentes y sin ser un friki creo que no lo hice del todo mal ¿o sí?
Una ultima cosa. confirmarme si realmente os faltan letras ¿ok?
Gracias de antemano... y gracias por elaborar esta pequeña/gran revista.
Ta lué!

MANUEL

¡Pues no está nada mal, para tratarse de un trayecto en tren! Sólo nos gustaría matizar un par de puntos: en primer lugar, ¡la gente a la que le gusta Tolkien y su mundo no tiene por qué ser friki! Cada uno tiene sus aficiones, y para nosotros, la verdad, ser aficionado al mundo de Tolkien es francamente divertido. Por otra parte, hemos comprobado de nuevo el segundo párrafo y no faltan letras... en cierto modo. Es decir: como la fuente utilizada es de origen inglés, no cuenta con caracteres acentuados ni otros caracteres que nosotros sí utilizamos, como "¿", o nuestra famosa "ñ". Precisamente estos dos caracteres deberían formar parte del texto, pero, al no estar disponibles, simplemente nos comimos el primero y sustituímos el segundo por una "n". Así que, si te parece, partimos la diferencia, ¿de acuerdo?



PARA HUMANOS: ¿DONDE SE PUEDEN ENCONTRAR EN EL WEB ESTAS FUENTES?
¿QUÉ HAY ESCRITO EN LAS FRASES QUE SIGUEN?

Enviad las respuestas a:
redaccion@hacker-journal.com

ECOECOOOOOOOOO

Holaaaaaaaa a tod@s. Pues estaba yo el otro día en la librería para comprarme una revista de informatica y os vi, la compré por curiosidad y me encantó. Tengo que decir que es una muy buena revista. Pero tengo un problema: sólo tengo del número 9 para alante y quería que me dijéseis como podría conseguir los números anteriores. Gracias, un saludo a toda la gente que hace esta revista y seguid así que lo estais haciendo muy bien.

JOSAFAT

Ya hemos comentado en ocasiones anteriores que, desafortunadamente, en estos momentos no tenemos una solución para proporcionar los números anteriores a nuestros lectores. Sin embargo, en el sitio web de la revista (www.hacker-journal.com) existe la sección "Secret zone" donde se encuentran los primeros números en formato PDF, que se pueden leer mediante el programa Adobe Reader (anteriormente Acrobat Reader). A su vez, este programa se puede descargar gratuitamente del sitio web de Adobe (www.adobe.com). Para acceder a la Secret Zone es preciso utilizar los códigos que publicamos en cada nuevo número de Hacker Journal. Consulta la página 3 para saber los códigos vigentes actualmente.

PROPUESTAS Y RETRASOS

¡salve!

mis agradecimientos a todos los escritores de Hacker Journal, no soy un profesional en ninguna área de computacion; de hecho nunca he tomado un curso, pero lo que he aprendido lo he hecho destruyendo mi computadora varias veces.
Pero ahora todo es diferente gracias a la revista aprendo mucho más sin ariesgar a mi compañera de todo agradecido.
Una cosa más: si les mando cosas de electrónica como kits o algo ¿lo publicarian?
Soy un joven de 17 años pero aprendo rápido y me gustaría compartir mis pocos conocimientos.
Si me responden haganlo al correo por favor porque el número lleva 3 meses de retraso.

MAYKIGHT O BALIC

Siempre es agradable saber que se es de ayuda a alguien, y especialmente cuando dedicamos un montón de horas a ello. Casi todos aprendemos mediante al antiguo y contrastado método del ensayo y error, lo que significa dejar el camino sembrado de cadáveres electrónicos... Pero en fin, un acierto de vez en cuando suele compensar todas las pérdidas.
Respecto a darte una respuesta, aquí la tienes, ¡con sus meses de retraso! Desafortunadamente, no podemos mantener correspondencia privada con nuestros lectores, por una simple cuestión de logística: son muchos vuestros mensajes, y resultaría imposible responder a todo el mundo. Por otra parte, es mucho más interesante publicar los mensajes posibles aquí, en estas páginas, de modo que todo el mundo pueda leerlos y aprender o formarse su opinión sobre los temas expuestos. Esperamos que lo comprendas. Finalmente, si tienes información que quieres compartir con los demás, puedes enviarla libremente, ya sea mediante esta sección o bien directamente en el sitio web de la revista.

EL C++ ATACA DE NUEVO

Estimados amigos de hacker journal:
Me ha encantado vuestro articulo de la seccion mail to: del ultimo numero, que habla del creador del c++ y su motivo.
Amigos de una página web argentina me han pedido que lo postee en su foro, por lo cual quería pediros permiso, así como el file con el texto integro para enviarlo.
Sin mas que contar, y agradeciendo su interés e intención, de despide de Vds...

ANTONIO

Amigo Antonio, publicamos aquel texto porque nos pareció realmente tan ilustrativo como a ti. Por lo que hemos podido averiguar, se trata de esos textos que rondan de vez en cuando por Internet, y la gente se los envía entre sí para opinar o simplemente pasar un buen rato. No estamos en condiciones de afirmar su veracidad absoluta, si bien la verdad es que leyéndolo uno llega a la conclusión de que, si no es cierto, merece serlo. En cualquier caso, se trata de un texto que nos mandó un lector a la redacción, de modo que estrictamente hablando no se trata de un texto propiedad de la revista. Por lo tanto, si tienes unos amigos que lo quieren publicar en su página web, por nuestra parte no hay ningún inconveniente. Eso sí, agradeceríamos que citaran que han obtenido el texto de Hacker Journal: al fin y al cabo, tenemos nuestra pequeña vanidad...
Por otra parte, de vez en cuando recibimos textos, la mayor parte de veces anónimos, que suelen dar que pensar. Ya que te gustó el de C++, no nos resistimos a reproducir aquí otro que nos ha llegado, sobre otra temática pero igualmente sugerente. ¡Que lo disfrutéis!

El ancho de via en los ferrocarriles de Estados Unidos es de 4 pies y 8,5 pulgadas. Es un numero bastante extrano.Porque se usa precisamente esa anchura? Pues porque asi es como se hace en Gran Bretana, y las vias americanas fueron construidas por ingleses expatriados.
Porque los ingleses usaban ese ancho? Porque los primeros ferrocarriles fueron construidos por las mismas personas que habian construido los antiguos tranvias y esta es la anchura que usaban.
Y porque ellos usaban tal cifra? Porque utilizaban las mismas plantillas y herramientas que se usaban para construir carruajes que usaban ese espacio entre ruedas.
Bien. Y porque los carruajes usaban esa extrana cifra de espacio entre ruedas?. Porque si hubiesen usado otra cualquiera se hubiesen roto en algun viejo camino ingles, ya que esa es la distancia entre las roderas.
Asi pues, ?Quien construyo esos viejos caminos con roderas? Las primeras carreteras de larga distancia en Europa (e Inglaterra) fueron construidas por el Imperio Romano para sus legiones y han sido usadas desde entonces.
Y las roderas en dichos caminos? Los carros de guerra de las legiones romanas formaron las roderas iniciales, que cualesquiera otros tenian que imitar por miedo a destruir las ruedas de sus carruajes. Ya que los carros fueron hechos para (o por) el Imperio Romano, eran todos iguales en cuanto a espacio entre ruedas.
El ancho de via standard en USA de 4 pies y 8,5 pulgadas deriva de las especificaciones originales para un carro de guerra romano. Especificaciones y burocracias viven para siempre. Asi pues, la proxima vez que te den unas especificaciones y te preguntes que culo de asno las pario, puede que estes exactamente en lo cierto, ya que los carros de guerra romanos se hicieron con el ancho justo para acomodar los traseros de dos caballos. Con lo que tenemos la respuesta a la pregunta original. Y ahora otra vuelta de tuerca... Hay una interesante coda a la historia acerca de anchos de via y culos de caballo. Cuando vemos una Lanzadera Espacial en su rampa de lanzamiento, notaremos dos grandes cohetes unidos a los lados del principal tanque de combustible. Son los llamados SRB (Solid Rocket Boosters) y son constuidos por Thiokol en su factoria de Utah. Los ingenieros que los disenaron habrian preferido hacerlos algo mas anchos, pero los SRBs han de ser enviados por tren desde la fabrica hasta el lugar de lanzamiento. La linea ferrea pasa por un tunel en las montanas y los SRBs han de caber a traves de ese tunel, el cual es ligeramente mas ancho que el propio ancho de la via, la cual es aproximadamente del ancho de dos traseros de caballo. Asi pues, el diseno de los cohetes impulsores del mas avanzado sistema de transporte del mundo fue determinado hace dos mil años por el ancho del culo de un caballo.

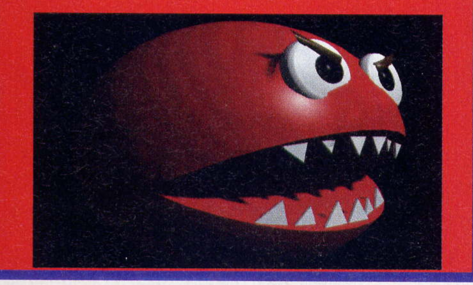
¡HOT!

CONGRESO INTERNACIONAL DE HACKERS DE BOLIVIA

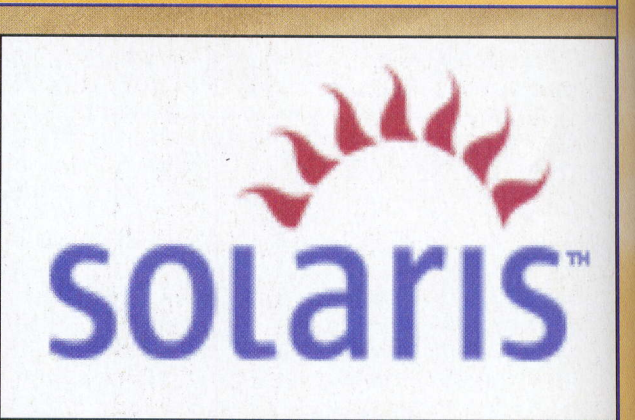
Este congreso internacional pretende convertirse en el evento más importante sobre técnicas de hacking y seguridad informática en toda Latinoamérica. Este evento tendrá lugar en la ciudad de Santa Cruz de la Sierra, Bolivia, los próximos días 2, 3, 4 y 5 de Marzo. El congreso reunirá a los mejores expertos de América y Europa, como Darío Forte, el presidente del capítulo europeo de la High Technology Crime Investigation Association, y colaborador habitual del instituto de seguridad informática de la NASA.
Teneis más información en su página web:
www.cih2k5.org

¿TE INSULTA TU ORDENADOR?

Si es así seguramente estas infectado por el virus Cisum.A.
Este sólo puede propagarse automáticamente en redes informáticas. En caso de que un usuario de una red ejecute un archivo con el gusano, éste se copia con el nombre ProjectX.exe.
Al mismo tiempo, muestra una ventana con el texto: "YOU ARE AN IDIOT", y ejecuta continuamente el mencionado archivo MP3 que el gusano ha generado previamente en el sistema. También finaliza procesos pertenecientes a aplicaciones antivirus y de seguridad informática, lo que deja a los equipos desprotegidos frente a otros posibles ataques . Además, crea varias entradas en el registro de Windows con el objetivo de asegurar su ejecución cada vez que se reinicie el ordenador. De todas formas no se han detectado más incidencias provocadas por este gusano.



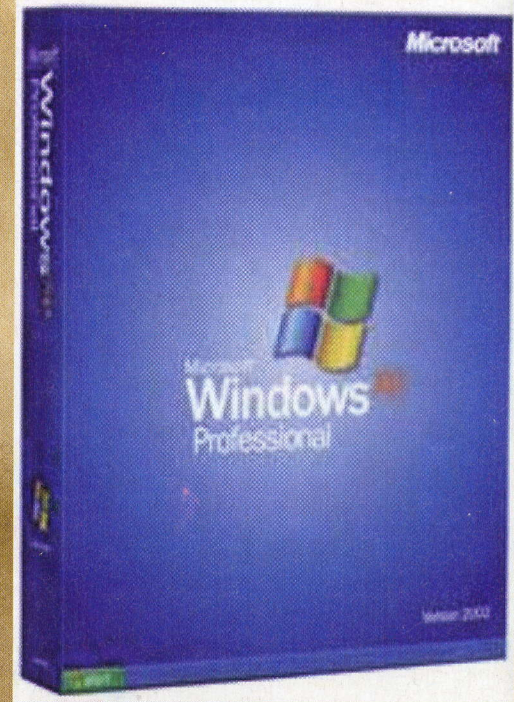
NUEVO OPENSOLARIS.ORG



La comunidad Open Source vuelve a estar de suerte. Otro de los grandes se apunta. Una vez más Sun colabora con el software libre como ya havia hecho en proyectos como OpenOffice.
El gigante informático Sun Microsystems ha anunciado definitivamente que planea compartir parte del código de su sistema operativo Solaris, su versión de Unix, y así confirma los rumores crecientes sobre su proyecto "OpenSolaris". La compañía espera que la apertura de su sistema operativo sirva para crear una comunidad de programadores en todo el mundo que trabaje con su software.
Solaris es una versión popular del sistema operativo Unix que, hasta ahora, ha conseguido aguantar el tipo en el mercado de servidores frente a la voracidad de Windows, de Microsoft. Pero la creciente popularidad de Linux, otra versión de Unix, constituye una amenaza de diferente naturaleza.
La primera parte disponible de Solaris ha sido la tecnología de análisis de rendimiento Dtrace. Otro código fuente de Solaris, como el sistema de archivos y tecnología de seguridad, se ofrecerán en el segundo trimestre de este año.
El código fuente de Solaris y las patentes están disponibles bajo la licencia Development and Distribution License (CDDL), aprobada por la iniciativa Open Source y está basado en la Mozilla Public License.
La compañía espera que la apertura de su software atraiga a los programadores y que éstos comiencen a desarrollar aplicaciones para "OpenSolaris". Un importante reto para este sistema operativo será la integración de código generado por una multitud de programadores con diferentes metodologías y que a menudo hablan lenguas diferentes.
www.opensolaris.org
www.sun.com

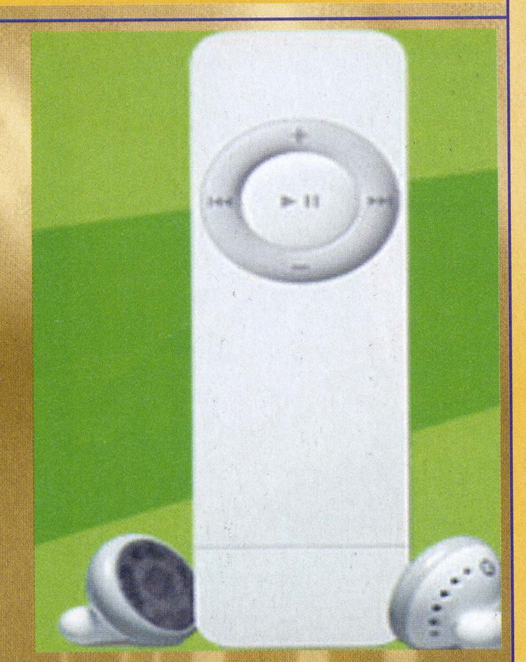
WINDOWS 64BITS

Algunas fuentes cercanas al gigante de Redmond están clamando que Microsoft planea presentar su sistema operativo de 64 bits para Intel y AMD el 29 de Abril. La versión definitiva de Windows XP 64 bits, afirman, comenzará a llegar a los fabricantes en Marzo, antes de que esté disponible en caja para el gran público.
Este sistema operativo que se ha visto forzado a dar el salto a los 64bits después de que algunos de sus competidores hayan publicado desde hace mucho tiempo versiones para estos procesadores.
Como coincidencia también destacamos algo que algunos ya tachan como más allá de la coincidencia: Intel también presentará oficialmente para esas fechas sus microprocesadores de 64 bits (incluyendo un Celeron 64). En contraste, recordemos que el AMD64 está disponible desde hace algo más de un año.
Veremos qué sorpresas nos depara Microsoft en los 64bits.
www.microsoft.com
www.intel.com



AUMENTO DE MÚSICA ONLINE

Parace que los negocios se han reordenado y reubicado. La venta de música a nivel tradicional se ha visto reducida a causa de la piratería. Eso sí, parece que en Internet las cosas son diferentes.
Las ventas de música en línea han resultado en que la industria discográfica por primera vez comience a captar ingresos verdaderamente importantes.
El miércoles 19 de enero, la organización IFPI informó que durante 2004 se descargaron de Internet más de 200 millones de títulos musicales comprados legalmente. La cifra se aplica a Estados Unidos y Europa y constituye un aumento del 1.000% con respecto a 2003.
La organización informó además que actualmente existen alrededor de 230 sitios web donde es posible comprar música totalmente legal. Hace un año sólo había 50 sitios dedicados a ese negocio.
Aunque todo indica que han llegado los buenos tiempos para la distribución comercial generalizada de música, la industria discográfica no ha contemplado reducir la intensidad de su campaña contra la piratería. IFPI afirmó categóricamente que seguirá demandando a quienes descarguen música ilegalmente de Internet.
La organización afirma que los 1.450 sellos discográficos afiliados sufren considerables pérdidas debido a la piratería, escribe Excite con base en información de AP.
Neogcios como el Apple Music Store parece que estan en auge.
http://www.apple.com/itunes/



VOIP GOOGLE

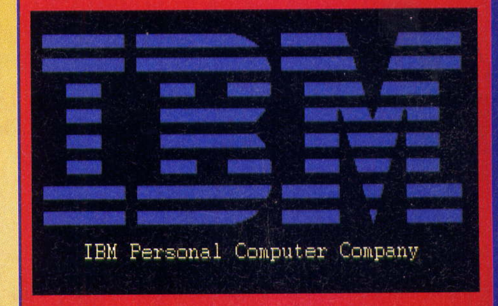
Parece que Google no tiene suficiente con ser el buscador líder en Internet y tiene que buscar más negocios en expansión. Después de lanzar su servicio (aún en fase beta) de búsqueda de video (http://video.google.com), ahora se dispone a atacar con nuevos servicios de Voz sobre IP.
VoIP es un protocolo de comunicación por voz a través de redes IP, las mismas sobre las que se sustenta Internet. El protocolo VoIP permite mantener conversaciones gratuitas de alta calidad a través de Internet e incluso con algo de infraestructura adicional y a un coste bajísimo realizar llamadas a teléfonos convencionales.
Un negocio en clara expansión, y con unas halagüeñas expectativas de futuro, cuyo principal exponente es actualmente el fenómeno "Skype".
Skype es un auténtico fenómeno de masas en clara expansión que ya es empleado por 54 millones de personas.
Según "The Times" Google está planteándose incluir enlaces a dicho protocolo en los resultados de sus búsquedas, de manera que por ejemplo cuando un usuario localice un sitio, el buscador le ofrezca junto con los resultados un enlace que nos permita "llamar por teléfono" al mismo.
Por otro lado, también se hace hincapié en un anuncio que publicó la semana pasada Google, buscando un especialista en redes de fibra óptica...
Sin duda, Google sigue pisando fuerte.
www.google.com



¡HOT!

IBM CEDE 500 PATENTES

IBM planea donar 500 patentes para libre uso de los desarrolladores de 'software', en lo que supone un giro en la estrategia de propiedad intelectual del gigante informático estadounidense, y un desafío para la industria de alta tecnología.
La cesión es válida para todo individuo, comunidad o empresa que trabaje en el desarrollo de software o que utilice 'software' de código abierto de acuerdo con la definición actual o futura de la 'Iniciativa Open Source', una organización sin ánimo de lucro que promueve el desarrollo del 'software' libre.
Conocidas personalidades del Software Libre la han considerado positiva aunque muchos insuficiente.
www.ibm.com



GOOGLE VIDEO

Google video es un nuevo servicio de este popular buscador que por medio de la búsqueda en el "closed captioning text" permite encontrar una amplia variedad de programas de televisión. Aparte de los resultados muestra capturas del video generando los primeros resultados del buscador que se complementan con thumbnails. Al ampliar la información de un resultado permite conocer más detalles de cada programa como las próximas fechas y canales donde será transmitido.
Una nueva innovación de la mano de google, que después de reflejar una pequeña bajada en sus "indices de audiencia" no puede dejar que esto se acentúe.

www.google.com
video.google.com



Un objeto semejante cabe en una aguja y puede inyectarse bajo la piel. Desde entonces seremos números, por radiofrecuencia.

TODOS SOMOS

Todos estamos acostumbrados a pasar por la caja del supermercado con el carrito lleno. Y a hacer cola esperando que los que van delante hayan acabado. De ahora en adelante, se acabó. Los productos serán leídos todos de golpe. Nada de cajeras: sólo un torno que se abre con la tarjeta de crédito, con la que se retira el dinero de la cuenta. De inmediato. Los nuevos sistemas de idenficación electrónica por ondas de radio mandarán al retiro sin duda alguna todas las barreras posibles. La nueva tecnología RFID (Radio Frequency Identification, idenficación por radiofrecuencia) ha superado en efecto la imaginación y tal vez la hallaremos hasta en la farmacia: junto con la vacuna antigripal, podremos adquirir el kit para la idenficación subcutáneo. Veamos cómo.

Todos numerados

El chip, de la empresa americana Find me (www.4verichip.com), contiene un código de 38 bits no alterable, integrado en la pastilla de silicio mientras se inserta. Echando cuentas, son posibles unos 490 miles de millones de números únicos que identificarán cada chip y por tanto cada persona en la que se inserte el chip.

La circuitería cabe casi toda en el chip, del tamaño de un grano de arroz, con una antena y un microcondensador para sintonizar. Nadas de pilas. El sistema se alimenta sólo de las mismas ondas de radio que recibe y para las que se ha sintonizado. Todo cabe en una cápsula de vidrio de 11 milímetros y 2,1 milímetros de diámetro. El tamaño justo para ser enhebrado en una aguja algo más grande de lo normal vendida en un kit estéril, con jeringas para la inyección subcutánea. La cápsula de vidrio es biocompatible y va untado con una sustancia que facilita la integración definitiva con los tejidos de nuestro organismo. Desde que se inserte en nuestro cuerpo seremos



Nueva frontera del wireless o gran hermano: ¿qué se cumple? Un contestador RFID no deja a salvo. Ahora es hasta inyectable bajo la piel

INQUIETANTE

Ciertamente, acercarse al cajero automático y retirar dinero de una cuenta corriente sin ni decir "soy yo" puede ser una gran comodidad. Pero puede abrir escenarios pavorosos. Quien quiera conocer de nosotros cada cambio, cada adquisición, cada costumbre sólo tiene que insertarnos el chip. Tal vez solapadamente, durante la anestesia de una intervención quirúrgica, por ejemplo. O la primera vez que vamos al dentista...
Más difícil, pero no imposible, es apoderarse de nuestra identidad: identificado el chip con una banal radiografía bastaría una minúscula incisión. Sin llegar a tanto, si en nuestros calcetines se inserta una etiqueta de RFID será ya probable reconocernos siempre. O ser siempre espiados.



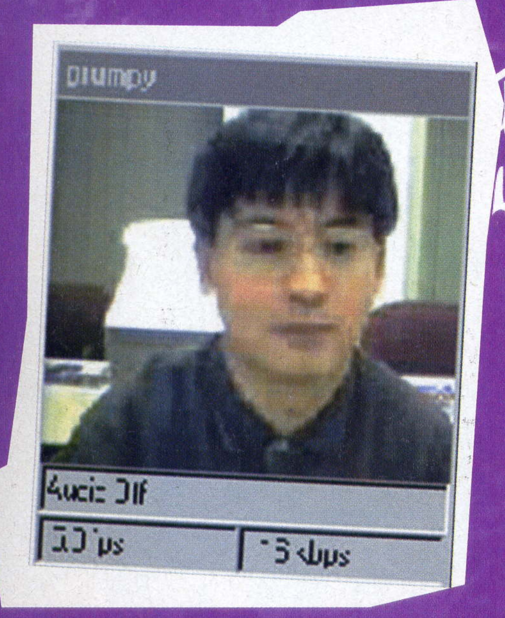
IDENTIFICABLES

numerados unívocamente y podremos entrar en el supermercado mientras una voz femenina automática enlazada a la base de datos nos acogerá con un "¡Buenos días, señor Pérez! Le hemos reservado algunos descuentos particulares en la sección de cosmética..." Por no hablar del paso por la autopista, la entrada en el puesto de trabajo, la entrada en un hospital... Si estamos en la base de datos se nos permitirá lo imposible. O nos vigilarán mejor...

Cómo protegerse

Uno de los problemas que se intenta resolver es la escucha a distancia. El principio sobre el que se basa RFID es muy simple: cuando el chip recibe la radiofrecuencia oportuna, absorbe la energía para autoalimentarse y responde con una emisión de radio que contiene el flujo de información en memoria. Quien sepa algo de radioelectrónica, con una antena direcccional puede ponerse a distancia para no ser visto y robar la información contenida en un chip cualquiera, abriendo nuevos escenarios de espionaje industrial, militar, sanitario y civil.
Un método para evitar la escucha a distancia, propuesto por el MIT, el Massachussets Institute of Technology, es cambiar el protocolo de base usado para la transmisión RFID y adoptar uno llamado "silent tree-walking". Un sistema propuesto por RSA, llamado de "pseudónimos", hace emitir a la etiqueta RFID identificadores que varían continuamente, por lo que la etiqueta parece informar a objetos diversos según el momento en el que se la interroga. Evidentemente quien tiene la lista de los "pseudónimos" no se deja engañar, pero quien no los tiene no podrá entender nunca de qué informa la etiqueta. Tal vez. Mientras tanto IBM ha invertido 250 millones de dólares en una nueva división que se ocupará de RFID y que emplea a más de mil personas. Un indicio nada despreciable de lo que nos sucederá cuando vayamos al supermercado en los próximos meses.

De la TEORÍA al



Todo lo necesario para hacer con éxito Voice over IP y hablar por Internet como si fuera una línea telefónica

Hemos hablado ya en algún número anterior del hardware mínimo para hacer Voice over IP y hacer viajar la voz por Internet: un PC con procesador 386, una tarjeta de audio full duplex y naturalmente una conexión a Internet. Son requisitos ampliamente superados por cualquier PC con menos de cinco años. A esto se le suma a veces una tarjeta de aceleración de hardware como PhoneJack o LineJack de Quicknet (http://www.quicknet.net/), capaz de comprimir el audio con gran eficiencia. Pero ahora hablemos de software.

El sistema operativo

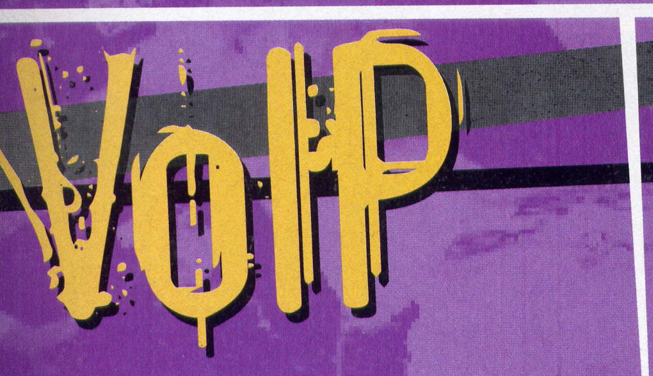
No hay problema en elegir Windows, Mac OS X o Linux: los tres van la mar de bien. Como mucho se tomarán elecciones distintas. En Windows los programas para VoIP son muchos: solo por citar algunos, Netmeeting,



En http://www.cisconetwork.net/html/index.php se encuentra este teléfono Cisco, ¡que hace Voice over IP y lo hace wireless!

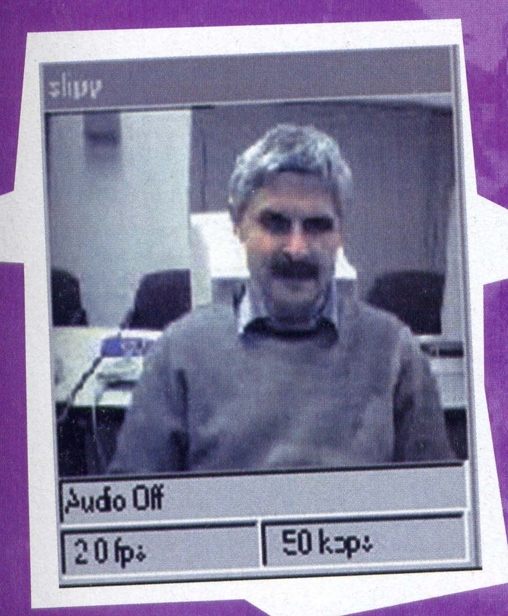
Internet Phone, DialPad. Quien use tarjetas Quicknet puede también optar a Internet Switchboard. Y naturalmente hay todo el software libre fácil de hallar gracias al trabajo del grupo OpenH323 (http://www.openh323.org/).

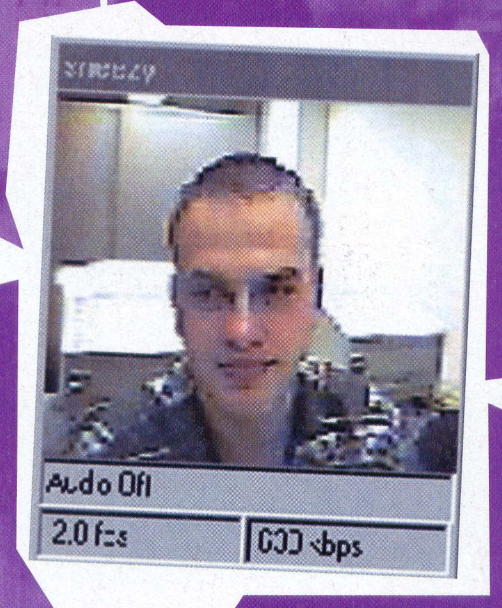
OpenH323 es la elección obligada en Linux. Algunos programas de la gama, como Simph323 u ohphone, funcionan también con las tarjetas de aceleración de hardware Quicknet. En Mac OS X, Apple ofrece iChat AV (http://www.apple.com/es/ichat) y se

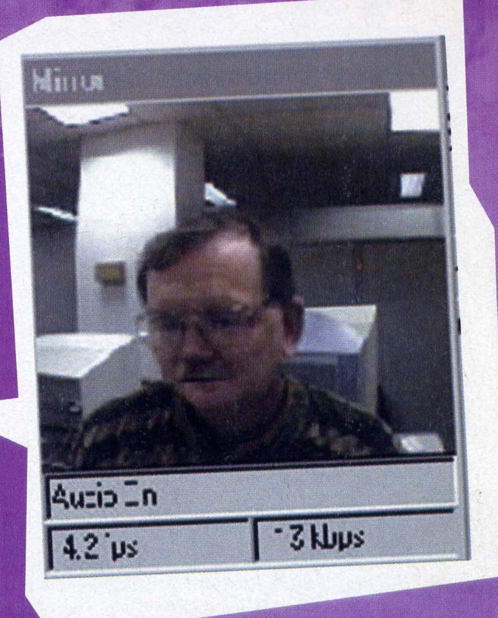


PROGRAMAS QUE USAN H.323

Microsoft NetMeeting - http://www.microsoft.com/windows/netmeeting/
Net2Phone - http://www.net2phone.com/
DialPad - http://www.dialpad.com/
Software open source (por ejemplo GnomeMeeting y Ohphone en el ámbito del proyecto OpenH323 - http://www.openh323.org/







puede usar todo el software existente para Linux. A veces ya está listo (véase http://xmeeting.sourceforge.net/ o http://www.ioxperts.com/apps_osXvideo.html), a veces hay que recompilarlos.

Software de gateway

Si se quiere hacer VoIP y llegar, cuando sea necesario, a líneas telefónicas tradicionales (PSTN, Plain Standard Telephone Network). En este caso se usa software de gateway, como Internet SwitchBoard (http://www.quicknet.net/) para Windows, o bien PSTNGw, fácil de hallar en el software OpenH323, que funciona en Windows pero también en Linux.

Servirá también el software de gatekeeper, o bien de gestión de todo el aparato. OpenH323 pone a disposición GNU Gatekeeper, en http://www.gnugk.org/, y Opengatekeeper, para Linux y Windows.

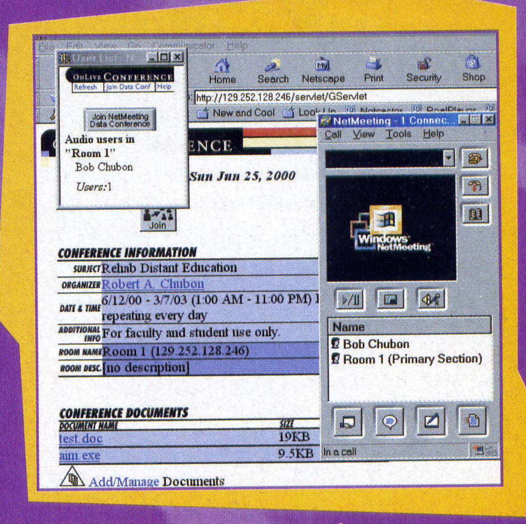
Un último software útil para resolver problemas es Phonepatch (http://www.equival.com/phonepatch), que soluciona problemas generados por la presencia de firewalls NAT. Phonepatch permite a los usuarios (dentro o fuera del firewall) llamar desde una página web. Cuando la aplicación presente en la página entiende que el destinatario de la llamada está listo, avisa a quien ha llamado y entonces se puede establecer la comunicación.

PROFUNDIZANDO

http://www.openh323.org/standards.html toda la documentación sobre los estándares de H.323

http://www.cs.columbia.edu/~hgs/rtp/h323.html también la documentación pero con ejemplos y guías rápidas

http://www.itu.int/itudoc/itu-t/rec/h/ todos los estándares de la serie H, del sitio ITU



↑ *Además de ser cómodo, poder usar la voz por Internet es una ayuda también para los minusválidos.*

Phonepatch, al contrario de otro software presentado aquí, es propietario, pero se puede descargar una versión demo que permite conversaciones de hasta tres minutos.

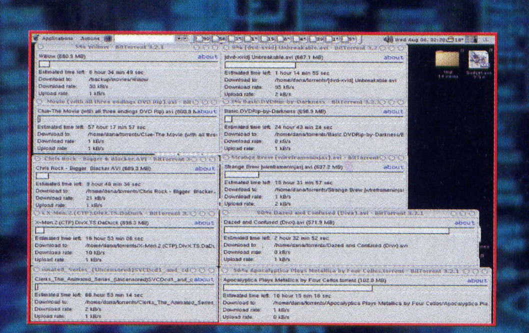
EN EL BAZAR

Exploramos los secretos de las redes p2p más usadas

Millones de usuarios de todo el mundo intercambian archivos de todo tipo conectando sus PCs mediante las redes peer-to-peer. Las discográficas y los productores de vídeo mienten: no es verdad que cuanto más adelanta la lucha contra la piratería se usan menos las redes p2p. Con los números en la mano, los usuarios de p2p crecen continuamente en todo el mundo, en una u otra red. Echamos un vistazo a los principales sistemas, que funcionan como si no vieran la mirada aterrorizada de quienes quieren controlarlo todo y limitar la libertad de Internet.
Los programas tienen versiones para diversos sistemas operativos, principalmente Linux, MacOS y Windows. Indicamos cómo descargar la versión de Windows, pero desde el sitio principal es fácil hallar los otros.

BITTORRENT

Es un sistema p2p que permite transferir archivos muy grandes simultáneamente a muchos usuarios. Cuando usamos BitTorrent en realidad no hacemos ninguna búsqueda de archivo en el PC de otros usuarios, como en el p2p normal, sino que accedemos a un servidor central donde hay una lista de todos los archivos transferidos recientemente. Las listas de servidores que guardan la lista de los archivos transferidos y dónde ir a buscarlos constituyen los archivos .torrent que son descargados antes que nada por el cliente. Desde ahí se interroga al servidor que lo dirige y después se carga el archivo desde donde se encuentra físicamente.



BITTORRENT

VERSIÓN ACTUAL: 3.4.2
LANZADA: abril 2004
DIRECCIÓN DE DOWNLOAD: http://bittorrent.com/download.html
TAMAÑO DE ARCHIVO: 2.226 KB
HOMEPAGE: http://bittorrent.com/

LIMITACIONES DEL Sp2

El Service Pack2 de Windows, SP2, y su seguridad crea muchos problemas a algunos programas p2p, como eMule , BitTorrent, SoulSeek y otros, porque limita las conexiones TCP simultáneas. Es posible remediarlo interviniendo en el archivo del registro yendo a cambiar el valor de una variabile que se llama DWORD y se localiza aquí:

System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: TcpNumConnections
Data Type: REG_DWORD (DWORD Value)
Value Data: 0 - 0xfffffe

FASTTRACK

La red FastTrack es la red de los populares programas Kazaa, Grokster e iMesh. Es una red descentralizada, lo que significa que no existe un nodo central de selección, sino que cada equipo se enlaza directamente a otro. Tiene la característica de crear un servidor provisional de indexado de los usuarios en cualquier equipo lo bastante potente que esté conectado. Por ello también nosotros podemos ser un servidor provisional, que facilita la busca aislando en subredes la enorme masa de usuarios que acceden normalmente con Kazaa. La estabilidad del conjunto ha llevado a FastTrack a ser utilizada por más de 4 millones de usuarios.

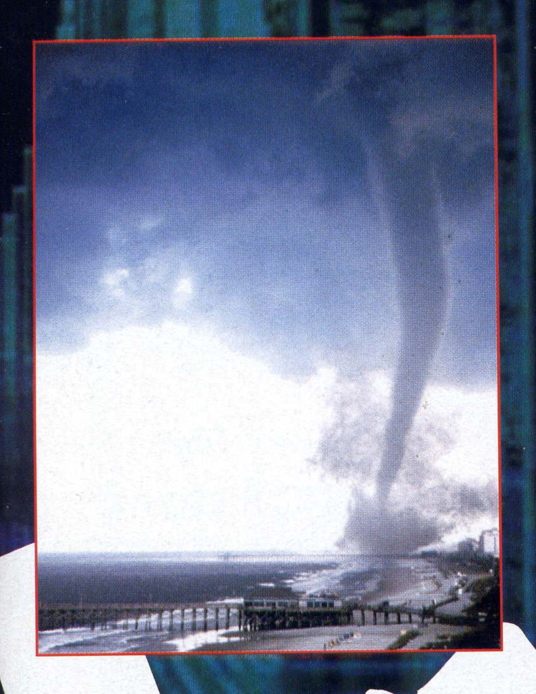


KAZAA

VERSIÓN ACTUAL: 2.6.6 (español), 2.7 (inglés)
LANZADA: abril 2004
DIRECCIÓN DE DOWNLOAD: www.kazaa.com/es/products/downloadKMD.htm
TAMAÑO DE ARCHIVO: 6,7 MB
HOMEPAGE: www.kazaa.com

DEL P2P
y los programas que las usan

TODOS LOS PROGRAMAS DE LOS QUE SE HABLA EN ESTE ARTÍCULO SE ENCUENTRAN FÁCILMENTE EN INTERNET



BITTORNADO

VERSIÓN ACTUAL: T-0.3.8
LANZADA: octubre 2004
DIRECCIÓN DE DOWNLOAD: http://www.bittornado.com/download.html
TAMAÑO DE ARCHIVO: 3,56 MB
HOMEPAGE: http://bittornado.com

BITCOMET

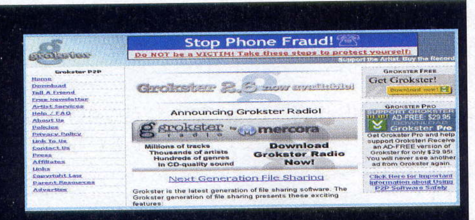
VERSIÓN ACTUAL: 0.56
LANZADA: septiembre 2004
DIRECCIÓN DE DOWNLOAD: www.bitcomet.com/doc/download.htm
TAMAÑO DE ARCHIVO: 1,649 KB
HOMEPAGE: www.bitcomet.com

OPENNAP Y WPNP

En la era de Napster, WinMX era un cliente apreciado y usado por número impresionante de usuarios. Hace unos años la red de Napster, OpenNap, fue acusada de tráfico ilegal de archivos mp3. Con la acción legal de la poderosa asociación de discográficas americanas, RIAA, sufrió un golpe mortal y siguió un periodo de caos. Hasta llegar la versión 2,5 de WinMX. Además de mantener el soporte a la difunta OpenNap, WinMX introdujo el protocolo de red WPNP (WinMX Peer Networking Protocol). Así, con una actualización de la versión, los más de 100 mil usuarios de la era de Napster se encontraron dentro de la nueva red, operativa de nuevo. Tras la versión 2,6 se han añadido más de 1 millón de usuarios, dando a esta red, a pesar de la RIAA, la fama de ser la mayor fuente de MP3 del mundo...

IMESH

VERSIÓN ACTUAL: 4.5 build 150
LANZADA: febrero 2004
DIRECCIÓN DE DOWNLOAD: www.imesh.com/download/download.php
TAMAÑO DE ARCHIVO: 3.16 MB
HOMEPAGE: www.imesh.com



GROKSTER

VERSIÓN ACTUAL: 2.6
LANZADA: febrero 2004
DIRECCIÓN DE DOWNLOAD: http://www.download.com/Grokster/3000-2166-10237041.html?part=dl-grokster&subj=dl&tag=button
TAMAÑO DE ARCHIVO: 251.27 KB
HOMEPAGE: www.grokster.com

WINMX

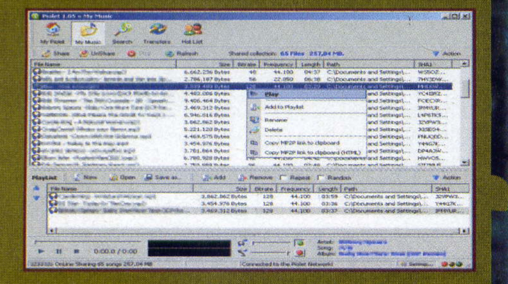
VERSIÓN ACTUAL: 3.53
LANZADA: julio 2004
DIRECCIÓN DE DOWNLOAD: http://dld91.winmx.com/8198751285/winmx353.exe
TAMAÑO DE ARCHIVO: 804 KB
HOMEPAGE: www.winmx.com

Manolito P2P network

Pura música. Solamente MP3. Nada de vídeo, .torrent, Dvd ni nada parecido. La red Manolito está dedicada sólo al intercambio de archivos MP3 y está muy controlada. Prácticamente no existen archivos incompletos o corruptos. Nació en 2001 En España por obra de un único programador: Pablo Soto. Como FastTrack, WinMX o Gnutella también Manolito es una red sin servidor central y por ello es más resistente a los ataques legales de las potentes asociaciones de casas discográficas americanas.

PIOLET

VERSIÓN ACTUAL: 2.0
LANZADA: marzo 2003
DIRECCIÓN DE DOWNLOAD: www.piolet.com/download/
TAMAÑO DE ARCHIVO: 504.36 KB
HOMEPAGE: www.piolet.com/

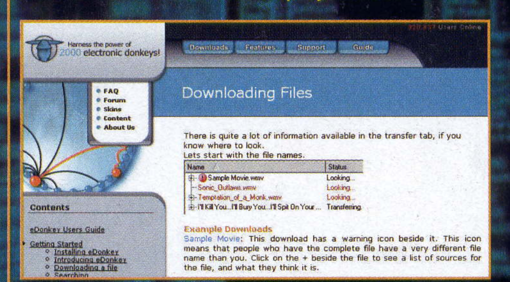


eDonkey2000

Es una red centralizada, y utiliza un servidor al que todos los clientes se refieren. Evidentemente al funcionar así se ve sometida a los ataques de la RIAA y de quien quiera limitar el intercambio de archivos p2p. Por el mismo concepto tuvo que cerrar Napster, que era una red centralizada en California. Para intentar evitar problemas de este tipo eDonkey no adopta un único servidor central, sino que hay varios y nunca tienen una sola ubicación precisa. Siempre se ha distinguido como la red para archivos de vídeo, películas, imágenes ISO de CD, y álbumes completos. Pesos pesados, vamos. Así se presenta como una alternativa a los Newsgroups más dispuestos o a las redes IRC. Parece que actualmente cuenta con más de 1 millón de usuarios.
Ahora incluye también la red OverNet y la nueva versión de eDonkey puede usar ambas redes. OverNet nació como una red descentralizada, alternativa a eDonkey2000. Pero esta última sigue viva gracias a la difusión de eMule, uno de los clientes que la usan.

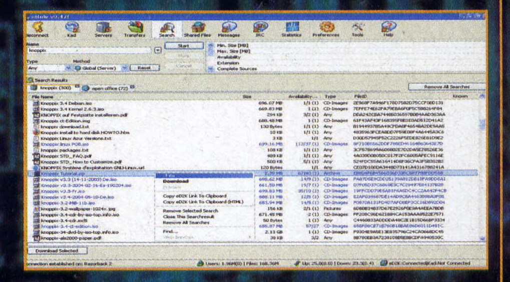
EMULE

VERSIÓN ACTUAL: 0.44d
LANZADA: noviembre 2004
DIRECCIÓN DE DOWNLOAD: http://www.emule-project.net/ home/perl/general.cgi?l=1&rm=download
TAMAÑO DE ARCHIVO: 4.058 KB
HOMEPAGE: www.emule-project.net



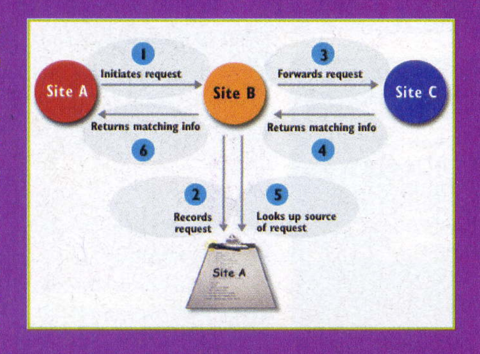
EDONKEY

VERSIÓN ACTUAL: 1.0
LANZADA: agosto 2004
DIRECCIÓN DE DOWNLOAD: www.edonkey2000.com/downloads.php
TAMAÑO DE ARCHIVO: 2,36 MB
HOMEPAGE: www.edonkey2000.com o bien www.overnet.com



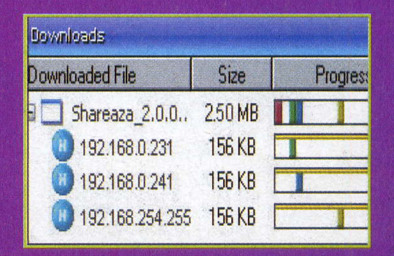
Gnutella

Una red descentralizada, por tanto sin servidores localizados en alguna parte. En cambio, también nuestro PC puede dar soporte a la red Gnutella, si es promovido a nodo super-peer, capaz de tener indexadas las direcciones de otros clientes ayudando con ello a dividir la red global en subredes más reducidas y más fácilmente consultables. Inicialmente fue desarrollada por Justin Frankle de NullSoft. Con el programa Shareaza se ha desarrollado una versión llamada Gnutella 2 que ha resuelto algunos posibles problemas de sobrecarga de la tecnología en la base de Gnutella, pero también es contestada por muchos usuarios como una traición a la idea de red original.



SHAREAZA

VERSIÓN ACTUAL: 2.1
LANZADA: septiembre 2004
DIRECCIÓN DE DOWNLOAD: www.shareaza.com/ ?id=download
TAMAÑO DE ARCHIVO: 3,56 MB
HOMEPAGE: www.shareaza.com/
NOTA: Soporta Gnutella2, Edonkey 2000 y BitTorrent.





LIMEWIRE

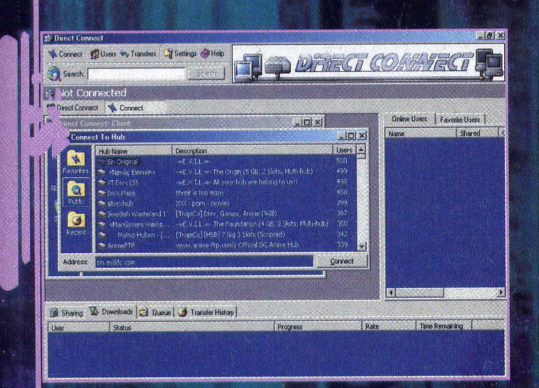
VERSIÓN ACTUAL: 4.0.8
LANZADA: septiembre 2004
DIRECCIÓN DE DOWNLOAD: http://www.download.com/LimeWire-International-/3000-2166-10132964.html?part=dl-limewire&subj=dl_int&tag=button
TAMAÑO DE ARCHIVO: 14,42 MB
HOMEPAGE: http://www.limewire.com/

DIRECTCONNECT

Es una de las redes más antiguas, muy semejante a la difunta OpenNap de Napster, pero tiene la particularidad de seleccionar el acceso concediéndolo sólo a quien es capaz de poner en común archivos por al menos 3 gigabytes. Esto lleva a una selección natural que desalienta a quien posee una conexión lenta. En efecto, los usuarios son sólo unos 400 mil, pero los archivos son muy seleccionados y en algunos hub también específicos (sólo imágenes, sólo música, sólo películas, etcétera). Como Napster es una red centralizada y esto la expone a los ataques de quien quiera indagar y profundizar lo que fluye por ella. Como en agosto pasado, cuando cinco equipos enlazados a DirectConnect cayeron en el punto de mira del FBI.

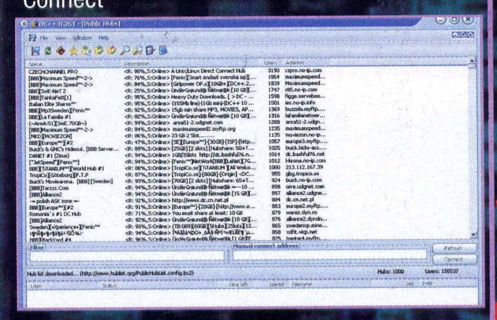
DIRECTCONNECT

VERSIÓN ACTUAL: 2.2.05
LANZADA: marzo 2004
DIRECCIÓN DE DOWNLOAD:
www.neo-modus.com/weeklies/ DCWeekly.exe
TAMAÑO DE ARCHIVO: 885 KB
HOMEPAGE:
www.neo-modus.com



DC++

VERSIÓN ACTUAL: 0.4034
LANZADA: marzo 2004
DIRECCIÓN DE DOWNLOAD:
http://prdownloads.sourceforge.net/dcplus-plus/DCPlusPlus-0.4034.exe?download
TAMAÑO DE ARCHIVO: 2322 KB
HOMEPAGE:
http://dcplusplus.sourceforge.net/
NOTA: es la alternativa OpenSource a Direct-Connect



SoulSeek

Es una red para quien no se conforma con las toneladas de MP3 que pueden hallarse en todas las demás. Si estamos buscando música electrónica, techno o dance, o una canción que hemos escuchado sólo en locales de Nueva York el sábado por la noche, aquí probablemente conseguiremos encontrarlo.
Se esponsoriza con pequeñas donaciones que proporcionan prioridad en los download.

SOULSEEK

VERSIÓN ACTUAL: 152
LANZADA: octubre 2003
DIRECCIÓN DE DOWNLOAD:
www.slsknet.org/slsk152.exe
TAMAÑO DE ARCHIVO: 738 KB
HOMEPAGE: www.slsknet.org



this script tests if the slsk server is up.

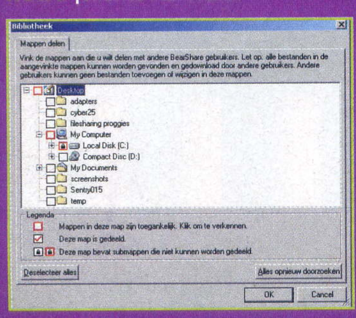
Slsknet.org :: Soulseek Board

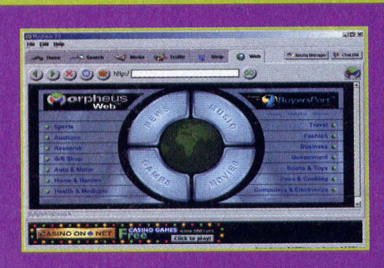
probing server... success.

the server is up and running!

BEARSHARE

VERSIÓN ACTUAL: 4.6
LANZADA: junio 2004
DIRECCIÓN DE DOWNLOAD:
http://download.bearshare.com/BSINSTALLIT.exe
TAMAÑO DE ARCHIVO: 3,12 MB
HOMEPAGE: www.bearshare.com
NOTA: ¡cliente Ad-ware!





MORPHEUS

VERSIÓN ACTUAL: 4.6
LANZADA: noviembre 2004
DIRECCIÓN DE DOWNLOAD:
http://www.download.com/Morpheus/3000-2166-10057840.html?part=dl-morpheus&subj=dl&tag=www
TAMAÑO DE ARCHIVO: 90 KB
HOMEPAGE:
www.morpheus.com
NOTA: ¡cliente Ad-ware!

GNUCLEUS

VERSIÓN ACTUAL: 4.6
LANZADA: noviembre 2004
DIRECCIÓN DE DOWNLOAD:
http://gnucleus.com/betagnuc/index.php
TAMAÑO DE ARCHIVO:
988.09 KB
HOMEPAGE: www.gnucleus.com

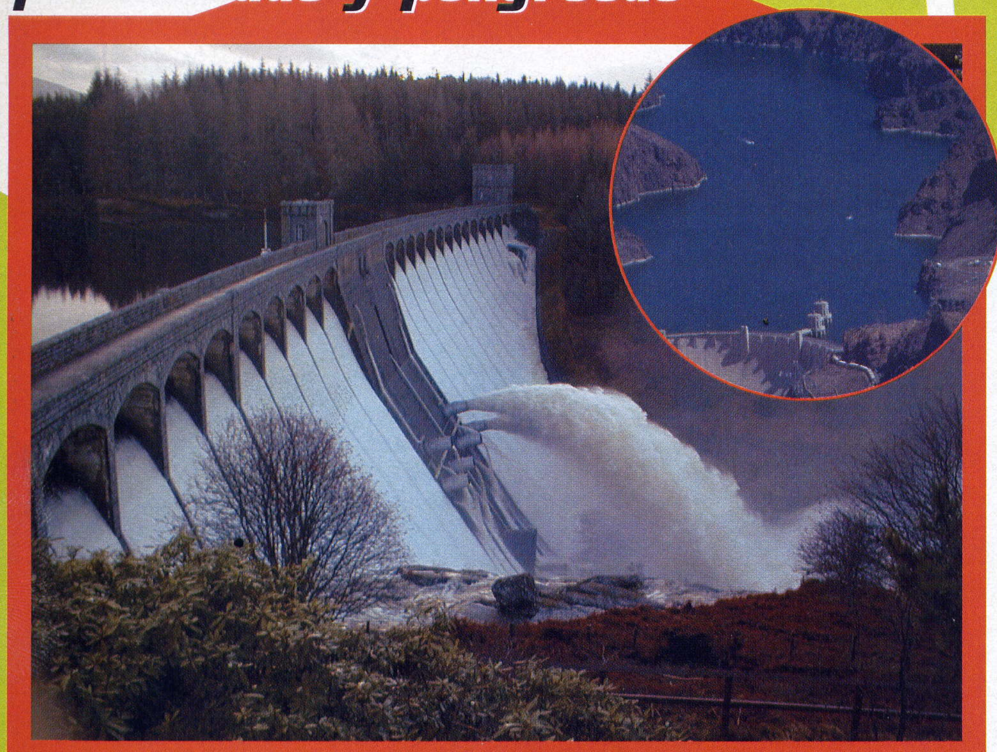


XOLOX

VERSIÓN ACTUAL: 2.0
LANZADA: mayo 2004
DIRECCIÓN DE DOWNLOAD:
http://www.download.com/3000-2166-10063575.html
TAMAÑO DE ARCHIVO: 79 KB
HOMEPAGE: http://www.xolox.nl/

Secretos del OVERFLOW

Una de las técnicas de ataque más practicadas y peligrosas



El buffer overflow se ha convertido en uno de los riesgos de seguridad más graves en Internet y en las redes locales. Está tan difundido porque los errores de programación se dan a menudo y no es difícil cometer uno de este tipo. No siempre se tiene acceso al código fuente, que permite aislar el problema, y no siempre quien tiene el código fuente sabe qué hace. ¡Por suerte estamos aquí!

Aviso: hay que entender al menos un poco el lenguaje C. ¡Una buena ocasión para aprenderlo! Hay muchas guías en Internet. También conviene saber algo de hardware. Los ejemplos se refieren a la arquitectura X86, en la que se basan todos los PC con Windows.

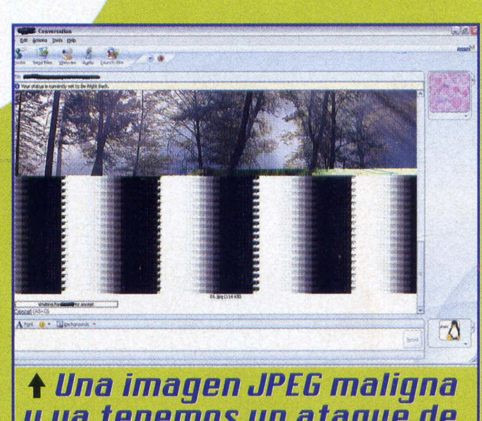
No estaba previsto

Explotar un buffer overflow significa enviar como entrada al PC atacado más información de la que éste está preparado para recibir. Los datos de más sobreescriben áreas de memoria no previstas y, si el ataque sale bien, son ejecutados por el procesador.

Para entender cómo sucede todo esto es preciso saber como se organiza la memoria RAM y, para empezar, qué son las páginas.

Todo es relativo (especialmente el direccionamiento)

Una página es una parte de memoria que usa su propio esquema de direccionamiento relativo. Direccionamiento relativo significa que el kernel (la parte fundamental del sistema operativo) destina la página a un cierto proceso en ejecución, pero no sabe dónde resi-



↑ Una imagen JPEG maligna y ya tenemos un ataque de buffer overflow.

BUFFER

de exactamente la página, o bien en qué chip de RAM se escriben realmente los datos. La memoria para los procesos se divide en tres: segmento de código, de datos y de pila.

En el segmento de código hay instrucciones en ensamblador (el lenguaje que habla el procesador), que se ejecutan. La ejecución no es necesariamente lineal. Puede haber saltos. Para ello existe un valor llamado puntero a las instrucciones. El puntero contiene la dirección de memoria donde se halla la próxima instrucción a ejecutar.

El segmento de datos aloja el espacio para variables y para buffers dinámicos. El segmento de pila se usa para pasar argumentos a las funciones y para almacenar las variables que las funciones devuelven. La base de la pila normalmente se halla al final de la memoria virtual direccionada por la página. La orden de ensamblador pushl añade información encima de la pila y la orden popl quita lo que está encima de la pila para insertarlo en un registro del procesador. Como en el segmento de código tenemos también aquí un puntero; el puntero de pila indica dónde se encuentra la cima de la pila.

Funciones

Una función es un trozo de código que se halla en el segmento de código y ejecuta una cierta tarea, tras lo cual el proceso sigue con el resto del código. Éste es un ejemplo muy banal de función en ensamblador:

```
DIRECCIÓN       CÓDIGO
0x8054321       pushl $0x0
0x8054322       call
                $0x80543a0
0x8054327       ret
0x8054328       leave
...
0x80543a0       popl %eax
0x80543a1       addl
                $0x1337,%eax
0x80543a4       ret
```

Con la instrucción pushl se pone un cero en la pila, a usar como argumento variable de la función, que se llama con call. La función toma la variable de la pila mediante popl y, una vez ha acabado, devuelve la ejecución a la dirección 0x8054327.

Ahora la pila está compuesta, de arriba abajo, por los buffers internos y la variable de la función, 32 bits del registro EBP y los 32 bits de dirección de retorno. La pila contiene además los argumentos pasados a la función, pero esto no tiene interés para un agresor.

La dirección de retorno, como hemos visto, es 0x8054327. En cuanto se llama a la función, se almacena de nuevo automáticamente en la pila. Esta dirección es el punto débil, que puede sobreescribirse para que apunte a cualquier otra área de memoria en caso de overflow.

En un próximo artículo veremos el ataque propiamente dicho.

VOCABULARIO

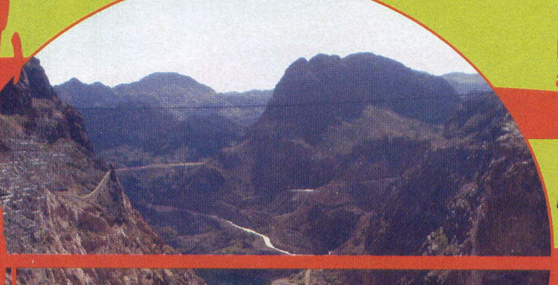
Pila: Estructura de datos en el que los datos son accesibles en el denominado esquema LIFO, que significa Last In First Out, o sea, el último que ha llegado es el primero en salir. El esquema LIFO es como una pila de libros en una caja: se puede tomar sólo el primer objeto, el de encima. Una instrucción push pone un objeto sobre la pila, un pop lo quita. Casi todos los procesadores tienen una pila.

→ *Gdiplus.dll: una biblioteca usada también para programar un Space Invaders en C*

↑ *Muchos aparatos de red incorporan controles para conjurar el peligro de buffer overflow.*

SP2 REMEDIA, PERO...

En la dirección http://www.us-cert.gov/cas/techalerts/TA04-260A.html se encuentra la descripción completa de una típica vulnerabilidad de buffer overflow en Windows. Se muestra una imagen JPEG creada por un agresor, el cual puede ejecutar código sobre el equipo de la víctima. El Service Pack 2 protege Windows, pero no las aplicaciones; si una de ellas se instala en el PC una versión vulnerable de gdiplus.dll, se corre peligro.



← *Si el agua rebosa en inglés es overflow.*

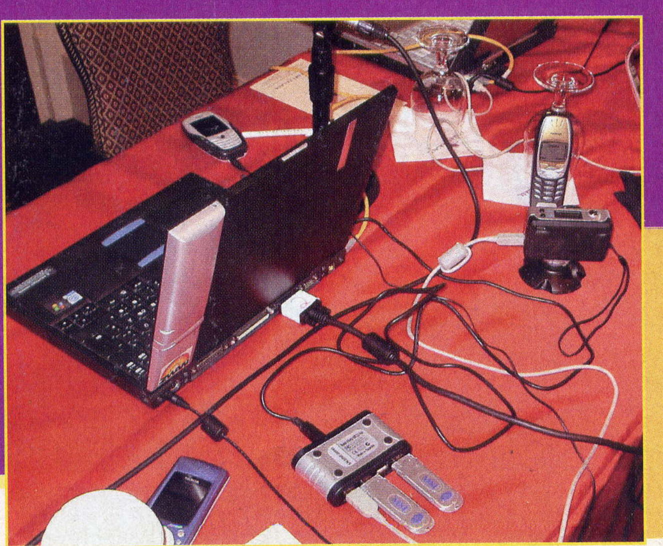
Bluebugging la nueva pesadilla de los móviles Bluetooth

Si pensábamos que los dialers eran un problema sólo de los teléfonos fijos, es que no hemos oído hablar aún del Bluebugging.

Imaginemos que podemos controlar un teléfono ajeno, como si estuviera conectado a nuestro portátil, exactamente como hacemos con nuestro teléfono. Resultado: estafa de llamadas telefónicas, invasión masiva de la intimidad y en el futuro también comprar a cargo de otros.
Si ahora le añadimos que todo esto ya es posible, desde hace más de seis meses, entonces estaremos ante uno de los mayores escándalos que ha afrontado jamás la telefonía.
Pero vayamos por orden, y empecemos por el vocabulario. Existen tres tipos distintos de interacción posible con un teléfono Bluetooth (ajeno):

Bluejacking

Esto es el envío de mensajes cuyo contenido va completo en el campo del nombre.
En este modo el mensaje aparece en el teléfono objetivo. En Gran Bretaña se usa normalmente como contacto sexual y muchos chicos y chicas hacen posible voluntariamente esta conexión para vivir la aventura.



Bluesnarfing

Detectado en noviembre de 2003, descubierto por A.L. Digital. Es posible copiar los datos de un teléfono: el registro de llamadas, el código IMEI, la agenda y las fotos; se pueden "actualizar" los datos en el teléfono objetivo.

Bluebugging

Divulgado por Martin Herfurt en marzo de 2004, con ocasión del CeBIT de Hanover. Es

Black Hat: en la mesa todo lo necesario para la demo, pero en realidad basta con un portátil y un dongle bluetooth

posible crear una conexión no autorizada a través de la conexión serie. Acceso completo al set AT del teléfono: se pueden mandar SMS, ejecutar llamadas telefónicas y programar el teléfono.Sus consecuencias quedan claras.

Los dos ponentes en DefCon fueron Adam Laurie <adam@algroup.co.uk>, jefe de seguridad de A.L. Digital, y The Bunker y Martin Herfurt <martin.herfurt@salzburgresearch.at>, responsable de I+D en el Salzburg Research Forschungsgesellschaft mbH. Ambos adivinaron la posibilidad de administrar los teléfonos bluetooth perjudicando al usuario, y pusieron un aviso en el foro de desarrolladores de bluetooth. Durante dos semanas no sucedió nada; entonces lo publicaron todo en el sitio de Slashdot. Resultado: Nokia se puso en contacto con ellos dos días despúes.

Así, se ha avisado a todos los fabricantes y es interesante ver cuáles ha sido sus respuestas ante la vulnerabilidad descubierta por los autores:

Nokia: contactó inmediatamente a los autores.



↑ *Martin Herfurt, a la izquierda, y Adam Laurie durante su intervención en BlackHat.*

TDK (desarrolla componentes para móviles): ha publicado un documento que explica que esto no es posible.

SonyEricsson: contactó con los autores y luego publicó un documento donde explica que esto no es posible.

Siemens y Motorola han mandado ejemplares de sus nuevos teléfonos a los autores para verificar su invulnerabilidad.

Si tenéis dudas sobre la posibilidad real de controlar a distancia un teléfono bluetooth, sabed que se realizó una demostración en las conferencias Black Hat y DefCon. Los autores, equipados con un portátil y un dongle bluethoot, empezaron por controlar el teléfono de un "cómplice" suyo sentado en la cuarta fila, el cual se levantó y se alejó por el pasillo, permitiendo a todos los presentes escuchar sus conversaciones. A continuación mandaron SMS a su teléfono desde otro teléfono también de un "cómplice" (para no cometer ningún tipo de delito).

Si con los dialers se llegó tarde, ¿qué queremos hacer con el control de los teléfonos bluetooth? Alrededor de un veinte por ciento de los teléfonos fabricados actualmente es vulnerable, lo cual significa que un malintencionado, por ejemplo cómodamente sentado en una mesa del bar de la estación de Chamartín en Madrid con su portátil con dongle bluetooth, puede localizar diariamente alrededor de doscientos teléfonos vulnerables y hacerles llamar a un número de pago, ¡con un rédito diario de más de 1.000 euros! Entre otras cosas, la conexión bluetooth no deja rastro en los log del teléfono y debido a la imposibilidad de duplicar los teléfonos GSM (aquí también habría MUCHO que hablar) los pobres desafortunados no pueden hacer más que pagar la abultada factura.

Laurie afirma que la mayor parte de las personas olvida apagar el Bluetooth y el modo de descubierta después de haber intercambiado información con un dispositivo (por ejemplo quien usa unos auriculares o un sistema de manos libres en el coche). Alrededor del veinte por ciento de los teléfonos descubiertos en la investigación eran visibles y vulnerable a algún tipo de ataque. En una prueba de dos horas hecha en Londres durante una hora punta, Laurie encontró 336 teléfonos bluetooth, 77 de los cuales eran vulnerables.

EN PELIGRO

Los teléfonos potencialmente expuestos a Bluesnarfing y Bluebugging:

Marca	Modelo	Firmware	Backdoor	Bluesnarfing modalidad Discoverabe	Bluesnarfing modalidad NO Discoverabe	Bluebugging
Ericsson	T68	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	No	No
Sony Ericsson	R520m	20R2G	?	Yes	No	?
Sony Ericsson	T68i	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	?	?
Sony Ericsson	T610	20R1A081 20R1L013 20R3C002 20R4C003 20R4D001	?	Yes	No	?
Sony Ericsson	T610	20R1A081	?	?	?	Yes
Sony Ericsson	Z1010	?	?	Yes	?	?
Sony Ericsson	Z600	20R2C007 20R2F002 20R5B001	?	Yes	?	?
Nokia	6310	04.10 04.20 4.07 4.80 5.22 5.50	?	Yes	Yes	?
Nokia	6310i	4.06 4.07 4.80 5.10 5.22 5.50 5.51	No	Yes	Yes	Yes
Nokia	7650	?	Yes	No (+)	?	No
Nokia	8910	?	?	Yes	Yes	?
Nokia	8910i	?	?	Yes	Yes	?
* Siemens	S55	?	No	No	No	No
* Siemens	SX1	?	No	No	No	No
Motorola	V600 (++)	?	No	No	No	Yes
Motorola	V80 (++)	?	No	No	No	Yes

* Modelos no vulnerables

++ El V600 y el V80 están en modalidad discoverable automáticamente cada 60 segundos cuando se encienden o se selecciona esta función del menú. Motorola ha comunicado que las nuevas versiones del firmware no tendrán este problema.

Origen de los datos: http://www.thebunker.net/release-bluestumbler.htm

CONEXIONES

http://agentsmith.salzburgresearch.at/
http://www.thebunker.net/release-bluestumbler.htm
Matthew Byng-Maddick <mbm@aldigital.co.uk>

HACKING

¿LINUX LIVE?

Linux Live (o mejor Live-CD) indica las distribuciones de Linux que pueden funcionar directamente desde el CD-ROM y no cuentan con instalación. Una distribución Live-CD muy famosa es Knoppix. La distribución que examinamos, Slax, se encuentra aquí: http://slax.linux-live.org

SECUENCIA DE BOOT

La secuencia de boot representa el orden en el que la BIOS busca los dispositivos arrancables de nuestro equipo. La secuencia de boot representa el orden en el que la BIOS busca los dispositivos arrancables del equipo. Un ejemplo: la secuencia 0- Floppy, 1-CD-ROM, 2-Hard Drive buscará arrancar primero desde el disquete, luego desde el CD-ROM y luego con el disco duro, y se para cuando halla un dispositivo arrancable. Ésta es la configuración más apta para ejecutar un Live-CD.

¿Y INITRD?

initrd (Initial Ram Disk) es un archivo de imagen ext2 con un filesystem Linux mínimo que sirve básicamente para cargar módulos del kernel antes de montar periféricos (por ejemplo para cargar los módulos para un cierto filesystem como reiser).

La distribución analizada es Slax versión 3.0.25. Veamos qué sucede en el momento del boot en un Linux Live y analicemos los modos de carga del sistema para actuar sobre los "puntos calientes" de la distribución.

Descomponer el ISO

Para poder analizar el sistema, ante todo tenemos que contar con una imagen iso del CD. Quien tenga el CD puede hacer un dump simplemente lanzando desde un shell Linux, como root, la siguiente orden:

```
# dd if=/dev/hdc of=/directory/deseado/slax.iso
```

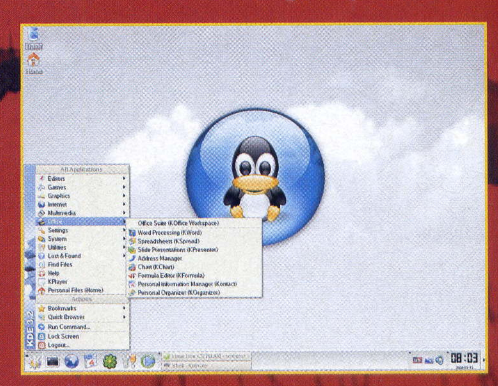
Evidentemente tendremos que sustituir /dev/hdc con el verdadero path de nuestro lector. Ahora estamos listos para abrir el iso. Desplacémonos al directorio donde hemos hecho el dump del iso, creamos un directorio y lanzamos las siguientes órdenes siempre como root:

```
# mount -t iso9660 -o loop slax.iso mydir
# cp -rp mydir slax
# umount slax.iso
# rm -rf mydir
# cd slax
```

Y he aquí que se nos presentan los archivos de la distribución, esperando a ser modificados...

En el boot

Si queremos ejecutar un live-cd hay que entrar en el BIOS y comprobar que el CD-ROM va antes que el disco duro en la secuencia de boot, sino será éste quien arrancará, a pesar de la presencia del CD en el lector.
A menudo los boot loader como LILO y GRUB son interactivos y permiten la carga de más OS (no es raro hallar un PC que tenga instalado Linux, con Windows e incluso también FreeBSD), pero en el caso de nuestro live-cd no. El boot loader de slax es isolinux, y está compuesto de los archivos isolinux.bin e isolinux.cfg. El primero es



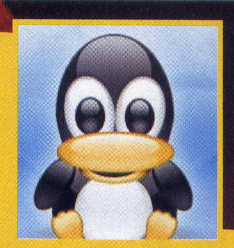
↑ *Linux Live: todo lo necesario, pero en un solo CD.*

el boot loader principal (podemos ver algunos posibles mensajes de error abriéndolo con un programa como biew), isolinux.cfg es el archivo de configuración. Leámoslo:

```
# cat isolinux.cfg
display splash
```



¿Descomponer y modificar un sistema Linux Live? Nada más simple... ¡para un hacker que se respete!



de un LINUX LIVE-CD

```
default slax
prompt 1
timeout 50

label slax
kernel vmlinuz
append max_loop=255
initrd=initrd.gz init=linuxrc
livecd_subdir=/ load_ramdisk=1
prompt_ramdisk=0
ramdisk_size=7777
root=/dev/ram0 rw lang=es
```

(éste no es el isolinux.cfg original sino uno modificado). La primera línea muestra el archivo "splash" (podemos modificarlo con un editor de texto), la siguiente define el label predeterminado, la otra habilita el prompt "boot:" que permite al usuario pasar parámetros adicionales al kernel. "label slax" indica la etiqueta que permite poner en marcha el OS del live-cd. La instrucción "kernel" define el archivo del kernel, al que se pasan algunos parámetros: los básicos van con la instrucción "append", los demás los pasa el usuario del prompt "boot:" y se describen en "splash". Analizamos los básicos: nos interesa sobre todo "initrd=" e "init=". Descomprimimos y montamos en loop el archivo initrd:

```
# gunzip initrd.gz
# mkdir initrd_mount
# mount -o loop,rw initrd
initrd_mount
# cd initrd_mount
```

Ahora podemos entrar y echar un vistazo. Destaca el valor del parámetro "init=", "linuxrc"; si lanzamos ls en el mount point del initrd podremos notar la presencia de un filesystem Linux completo y un script Bash llamado linuxrc. Cuando lo abrimos vemos que ante todo se importa otro archivo de bourne shell-script(functions) con algunas funciones usadas dentro de linuxrc, y podemos llegar a entender todas las operaciones hechas por este archivo: la creación de un filesystem virtual, el descompactado de las imagenes, su copia en el filesystem recién creado, el chroot, es decir, el cambio del directorio de root y en fin el arranque del sistema recién desempaquetado, al terminar lo cual se nos presentará una pantalla de introducción y el prompt de login, lo que significa que nuestro Linux Live está listo para obedecer nuestras ordenes.

```
#!/bin/sh
. ./functions
export PATH=/usr/sbin:/usr/bin:/sbin:/bin:/:.

# storage files
MOUNTS=/mounts.log
MNTORDER=/mnt.order
INSORDER=/ins.order
STGFILE=/mnt/tmp/ovlfs.stor

# paths
LIVECDDATA=/mnt/mnt/livecd
IMGRO=$LIVECDDATA/imgro
IMGRW=$LIVECDDATA/imgrw
CP2RAM=$LIVECDDATA/cp2ram
CHANGES=$LIVECDDATA/changes

# init script, absolute path for chrooted filesystem
LINUXINIT=/tmp/init

header "linuxrc-start"

echo "creating root filesystem in /mnt"
mount -t tmpfs -o size=90% tmpfs /mnt
mkdir -p /mnt/{bin,boot,dev,etc/X11,home,lib,mnt,opt,proc,root,sbin,tmp,usr,var/run,var/lock}
mkdir -p /mnt/mnt/{ramdisk,livecd}

# touch to avoid "overmounting" by ovlfs, which could sometimes cause errors
# with locking. For example /etc/mtab locking or /root/.Xauthority locking
touch /mnt/{etc,root,tmp,var/run,var/lock}/.lock_enable

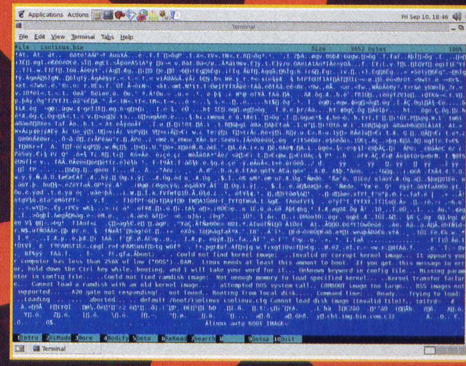
mount -t proc proc /proc

DEBUG="`cmdline_value debug`"
```

EL CONTENIDO DE LINUXRC

No hemos terminado...

Hasta ahora hemos analizado el boot de la distribución, de fundamental importancia para no cometer errores durante la modificación del live-cd. En un próximo articulo analizaremos la disposición del filesystem final en el live cd, cómo se montan los directorios (/usr, /bin, /lib, /etc.) y los métodos de creación de los iso. Con los conocimientos adquiridos podemos divertirnos modificando los parámetros en isolinux.cfg y en linuxrc, crear los iso con la utilidad create_bootiso (se encuentra en el root del filesystem iso principal) y ver qué sucede. Para probar el iso recomendamos un emulador como Bochs, que podemos hallar en SourceForge.net.



↑ *Los potenciales errores del bootloader Isolinux.bin.*

Misterioso archivo espía

Son cada vez más frecuentes las confusas señales de quien dice ver su propio PC comprometido en grandes duplicaciones de archivos llegados de Internet, con gran derroche de tiempo y, evidentemente, con gran sospecha de un comportamiento anómalo.

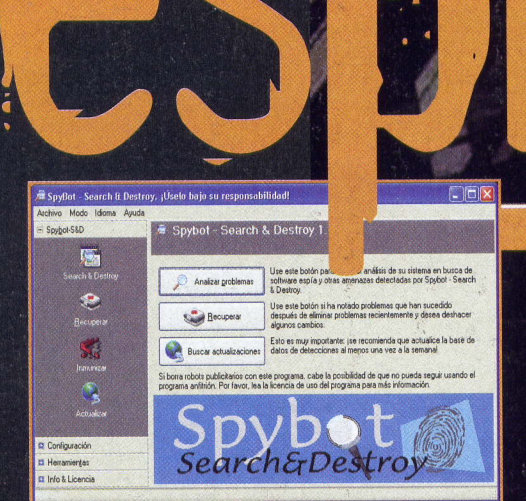
Como si nuestro PC usara datos de la red, o no, sin motivo. Hasta se han detectado flujos de datos hacia direcciones concretas. Por ejemplo hacia www.comcast.com, www.rr.com, www.bb4.org, etc. ¿Es esto normal? Evidentemente no, sobre todo si indagamos la fuente de un comportamiento tan extraño...

Spyware y parecidos

La primero que hay que hacer, es aislar al culpable del comportamiento sospechoso en el PC. Un buen software que aisla y destruye el malware puede irnos bien. Spybot es el que está más en boga: simple de usar, actualizado, veloz y eficaz en muchos frentes abiertos del PC, desde ejecutables hasta entradas de registro.

Lo podemos descargar de http://security.kolla.de. Lo instalamos, lo actualizamos inmediatamente en la misma fase de instalación y ejecutamos un análisis de todo. Si hay un spyware hemos resuelto el problema y podemos destruirlo con el mismo Spybot. Luego tendremos que preguntarnos cómo entró y cerrar todas las vías de agua del sistema, para no seguir en situación de riesgo. Probablemente muchos problemas los podemos resolver fácilmente aplicando un cortafuegos de software. O bien, considerando que somos usuarios de Windows y estamos a punto para aceptar las consecuencias, es la ocasión para descargar el Service Pack 2, que tiene un cortafuegos interno bastante eficiente.

Si tenemos Windows XP, probamos a instalar SP2 y su parche aparecido hace poco. Un paquete, Microsoft, ciertamente, pero menos malo con respecto a versiones pasadas. Al menos aumenta visiblemente la estabilidad del sistema.



Un clásico antiespía: Spybot al ataque

NDISUIO.sys

Si todo este proceso no basta, porque no se señala la presencia de spyware y todo parece normal, podemos concentrarnos en algún archivo específico presente en el sistema operativo. NDISUIO.sys es uno de ellos. En opinión de muchos usuarios y de discusiones en diversos foros, el tráfico irregular de datos en nuestro equipop parece generado precisamente por este archivo.

En efecto, NDISUIO.sys es un controlador de Microsoft, y no un spyware. O al menos así se describe. Algunos en cambio afirman que podría tratarse de alguna versión de este archivo un poco demasiado parlanchina, y que vale la pena desactivarlo de todos modos.

Otros están convencidos de que si este archivo es un soplón, es culpa de algún malware, todavía no localizado, que altera un controlador normalísimo de Microsoft que, por sí mismo, no tiene nada que ver con el Gran Hermano.

¿Qué hacemos?

Microsoft describe el servicio en esta dirección: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wceddk40/html/cxrefndisuser-modeiodriver.asp donde, en la práctica, dice que NDIS

¿QUIÉN QUIERE PROBAR?

La solución al misterio de NDISUIO.sys no es fácil, pero para los más curiosos el sitio donde empezar a hacer averiguaciones es éste: http://www.ndis.com/pcakb/KB01010301.htm

Si preferimos leer experiencias de usuarios sobre el tema, éste es el sitio adecuado: http://forum.defcon.org/archive/index.php/t-2142.html



Mientras se usa Windows XP puede ocurrir que el flujo de los datos desde y hacia la red aumente vertiginosamente. ¿Qué está sucediendo?

User-mode I/O (NDISUIO) es un controlador de protocolo que soporta el envío y la recepción de datos vía Ethernet utilizando ReadFile y WriteFile.
Como controlador de protocolo, NDISUIO dice cómo establecer la comunicación entre los controladores de la red Ethernet, cómo adecuar los filtros de paquetes y cómo recibir y enviar datos.



↑ *Desactivamos NDISUIO.sys mientras estamos a tiempo*

He aquí algunas de las cosas que puede hacer el controlador de NDISUIO:
- autenticación de usuarios para los dispositivos WiFi 802.11
- recuperar valores de la potencia de señal
- envío y recepción de paquetes mediante las puertas de enlace
etcétera, etcétera.

Es pues un verdadero generador de flujos de datos, muy utilizado si activamos la comunicación WiFi.

¿Y si no la utilizamos? Entonces podemos desactivarlo, para evitar errores.

Cómo desactivar el archivo

He aquí el procedimiento para desactivar el servicio NDISUIO.SYS:

Inicio-> Ejecutar -> Regedit -> Aceptar

Se abrirá el editor del registro de sistema.
Buscamos la clave:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndisuio

Cambiamos el valor de "Start" de

0x00000003 a 0x00000000

Reiniciamos el sistema.

Cómo reactivarlo

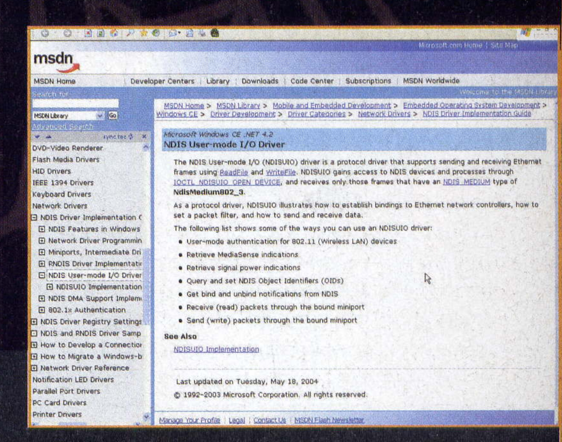
Procedimiento para activar el servicio NDISUIO.SYS:

Inicio -> Ejecutar-> Regedit -> Aceptar

Se abrirá el editor del registro de sistema.
Buscamos la clave:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndisuio

Cambiamos el valor de "Start" de 0x00000000 a 0x00000003



↑ *En el sitio de Microsoft se describe (en inglés) la función de NDISUIO.sys*

Reiniciamos el sistema.

Utilizando este método el controlador NDISUIO.sys deja de estar activo y ya no engendra más tráfico, ahorrando tiempo de proceso y, si implicaba a Internet, ancho de banda para nuestro uso y consumo. Hemos probado alguna funcionalidad de Windows, como "Actualización automática", y esta desactivación no parece crear ningún problema. Desgraciadamente la desactivación de NDISUIO.sys no permite el uso de sistemas Wireless.

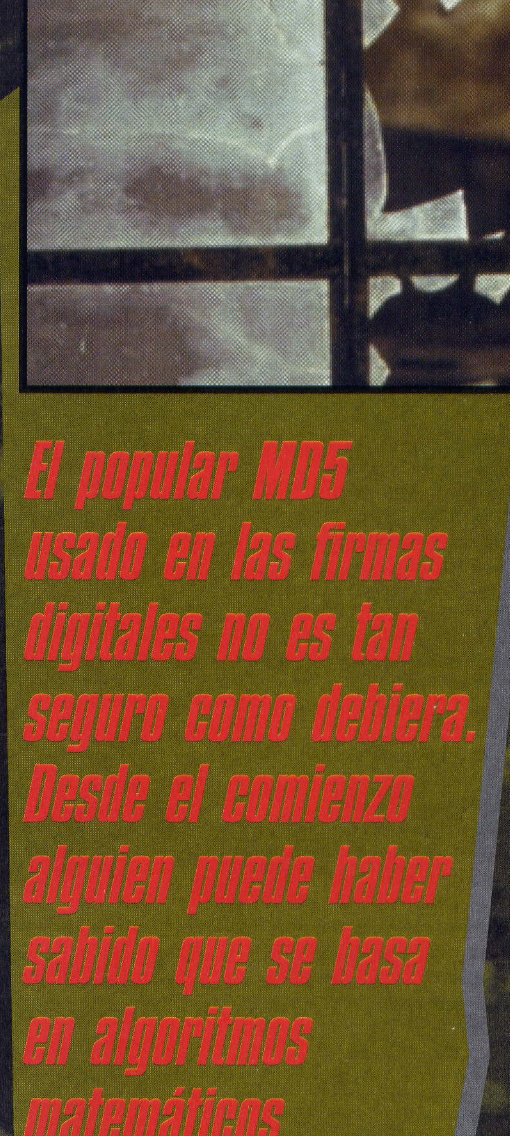
FALLOS A RÁFAGAS

en los ALGORITMOS DE CIFRADO

MD5 es una especie de "síntesis" de cualquier documento que se le pase. En el sentido que mediante un cálculo matemático toma un mensaje de longitud arbitraria y produce como resultado una especie de huella digital del documento de 128 bits y, creíamos hasta hoy, único. Podemos hallar una descripción completa en la dirección www.faqs.org/rfcs/rfc1321. Cuatro investigadores chinos han escrito un documento en el que se demuestra, literalmente, cómo tomar el pelo al algoritmo. Así, de dos documentos diferentes en realidad es posible obtener dos firmas iguales: lo que evidentemente hace caer de golpe toda posibilidad de utilizar MD5 para usos mínimamente serios.

¿Qué podría suceder ante un juez, si pudiéramos demostrar que alguien puede falsificar la firmar pasando un documento como nuestro? ¿O qué puede pasar si descargamos un archivo de Internet creyendo disfrutar de las garantías de la cadena MD5, y en cambio en realidad descargamos un troyano destructivo hecho adrede para tener la misma firma que el archivo que buscamos? Si el documento de los chinos se considera válido, miles y tal vez millones de archivos MD5 y sus archivos de origen deberían eliminarse del web, revisarse y sustituirse por algo más seguro. Menuda movida.

Pero hay más. Este año se ha demostrado, por parte de Eli Biham y Rafi Chen, investigadores israelitas, que el aún más famoso algoritmo SHA-1, considerado seguro, tiene puntos vulnerables hasta ahora desconocidos. Esto implica, por ejemplo, que ni los populares programas PGP y SSL pueden considerarse ya seguros. SHA-1 ha sido incluso certificado como algoritmo seguro por el instituto nacional de estándares americano, produciendo un cadena de salida del documento de 160 bits. Sin embargo es vulnerable.



El popular MD5 usado en las firmas digitales no es tan seguro como debiera. Desde el comienzo alguien puede haber sabido que se basa en algoritmos matemáticos inseguros.





MD5 y SHA-1 son algoritmos reconocidos hasta ahora prácticamente a prueba de bomba, porque un solo cambio en el mensaje original debe producir una huella digital completamente distinta, ya se trate de un correo o de un archivo del sistema operativo.
Pues resulta que no. Ahora ya no es posible decir con seguridad que son algoritmos útiles para la seguridad. En sustancia es como si ya pudiéramos clonar las firmas digitales, con una operación que produce las denominadas colisiones.
Siempre se ha sabido que ningún algoritmo puede ser declarado completamente seguro. Pero siempre se ha pensado que esta carencia podría derivarse del tiempo necesario para crear un resultado disparatado, o sea una colisión. Si se puede hacer algo, pero se emplea un tiempo muy largo, tan largo que el resultado no es utilizable por quien ha empezado el trabajo de ataque, es evidente que difícilmente sirve de algo. Por ello el algoritmo se puede considerar seguro.

El sistema SHA-1 exige al equipo que lo calcula que pase las rutinas que lo constituyen al menos 80 veces, hasta crear la firma unívoca. Biham, el investigador israelita, ha podido duplicar una firma digital en sólo 30 de los 80 pasos previstos. Dejando estupefacta a la comunidad internacional.
Si profundizando en las vulnerabilidades de SHA-1 se descubrieran agujeros análogos a los que han hecho abandonar la anterior versión SHA-0, bastaría una pequeña red de PCs actuales para romper en un tiempo razonable cualquier aplicación basada en este algoritmo.

Los problemas de MD5 pueden implicar a muchos servidores, como todos los que montan Apache Web Server, que usa MD5 para garantizar a los usuarios que el código fuente de docenas de mirrors contienen archivos idénticos a los originales y son por ello seguros. Sistemas como Solaris Fingerprint Database, que garantiza la seguridad de los archivos del sistema operativo Solaris, basado en MD5, pueden encontrarse en la embarazosa situación de tener que dar explicaciones a los usuarios sobre cómo garantizar la unicidad de los archivos ante el uso de un algoritmo que crea clones con notable facilidad.
Con el algoritmo MD5, según los investigadores, unas horas en un PC estándar bastan para crear clones de cualquier firma digital. Que estamos en una situación insegura, se podía suponer. Que lo estemos a tal nivel, es verdaderamente preocupante.
Los documentos sobre la vulnerabilidad son de dominio público; dentro de poco alguna organización lo aprovechará para realizar ataques masivos. Al tiempo.



¿Cómo habla el OSI así?

¿Cómo lo hacen ordenadores tan diferentes para entenderse entre sí? Daremos una explicación, que usa términos como "Nivel físico" o "Nivel de transporte". Entenderlo nos llevará más lejos

Estar en un campo de fútbol no significa poder jugar a fútbol. Es necesario que los dos equipos conozcan las reglas, sepan cómo empezar a jugar, nombren a un árbitro para calmar las discusiones... Lo mismo vale para nuestro ordenador. Tener una tarjeta de red no quiere decir que si lo conectamos con otro, logren hablarse. Y menos si usan sistemas operativos o aplicaciones diferentes. Es preciso que ambos respeten las mismas reglas.

Los árbitros internacionales, o sea las organizaciones de estandarización ISO, han intentado poner de acuerdo a todos creando un conjunto de reglas, o sea un modelo, llamado Open System Interconnection: OSI, en resumen.

El modelo al desnudo

OSI se compone de siete estratos, cada uno de los cuales tiene su función específica y habla con los niveles que tiene por encima y por debajo. Cuanto más se baja de nivel, más primitiva resulta la comunicación. El primer nivel es el físico, los cables o los medios de transporte usados para transferir los datos. El nivel más noble, en el séptimo piso, está dedicado a charlar con las aplicaciones que usemos.

En medio, está por ejemplo el cifrado y todas las otras cosas que se quieran hacer. El concepto de base es que cada nivel hace cosas que no requieren cambios en los niveles superior e inferior. Al dividir así el problema de la comunicación entre dos ordenadores, es más fácilmente manejable. Basta cambiar el nivel adecuado y sólo ése, y listos.

Es un poco como decir, por ejemplo, que podemos enviar el correo electrónico por cable ADSL o por fibra óptica, o a través del módem, sin tener que cambiar de programa.

Viéndolo queda más claro.

Veamos en la práctica qué sucede.

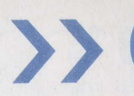
OSI CONTRA TCP

¿Dónde se encuentran los protocolos como TCP (Transmit Control Protocol) o IP (Internet Protocol) en el palacio de los siete pisos OSI?

En este esquema podemos ver las correspondencias. Los ataques DoS a base de ping, por ejemplo, se dirigen al nivel tres. Por su parte, los exploit que en cambio afectan al protocolo TCP, se dirigen al nivel cuatro. La ordenación del asunto afecta también a los ataques.

HACKER JOURNAL

↑ La transmisión empieza en el nivel 7. Tenemos que enviar el mensaje "Hacker Journal", con una aplicación cualquiera, como el correo electrónico.




HACKER JOURNAL

HACKER JOURNAL

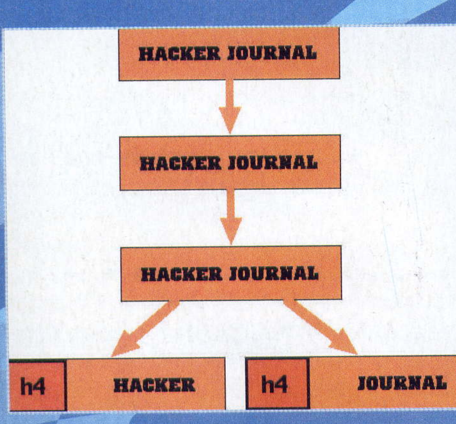
El mensaje se prepara en el nivel 6 para ser aceptado en los niveles más bajos. La compresión y el cifrado se colocan aquí.

HACKER JOURNAL

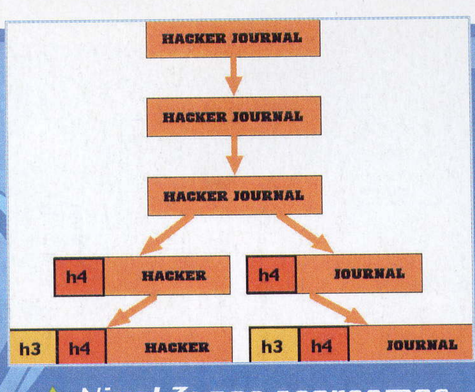
HACKER JOURNAL

HACKER JOURNAL

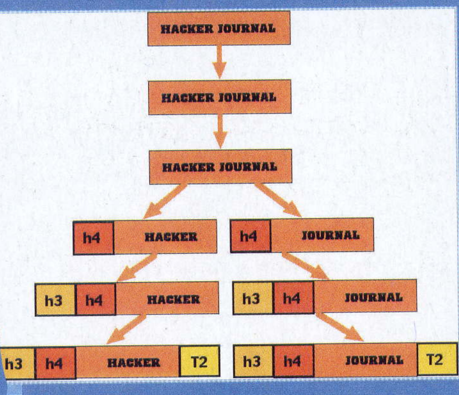
Prácticamente ningún cambio significativo. En este nivel, el 5, se regula sobre todo el flujo de datos.



Seguimos dentro del equipo que e stá transmitiendo. En el nivel 4 el dato se divide en paquetes más simples y se añade una cabecera a cada paquete. Las cabeceras contienen números secuenciales y otros datos de control.



Nivel 3: nos acercamos rápidamente a la verdadera transmisión de los paquetes. Aquí se añade otra cabecera, que servirá para enrutar el paquete hacia su destino.



Estamos listos, se añade una cola para adecuar los paquetes al sistema que transportará efectivamente los datos. Debajo de este nivel, los paquetes estarán ya en algún medio físico que los deberá transportar, ya sea por las ondas de un dispositivo WiFi o el cable de la red Ethernet.



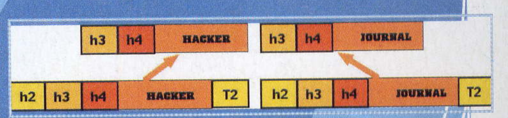
El mensaje alcanza un equipo en la red en la que se está conectado. Este equipo comprueba que el mensaje sea para él. No lo es, por lo que pasa el mensaje al nivel 2.



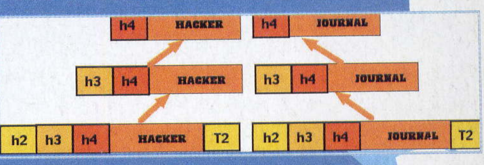
El nivel 2 lo reenvía al nivel físico para que siga su camino hacia el equipo de destino.

h2 h3 h4 HACKER T2 h2 h3 h4 JOURNAL T2

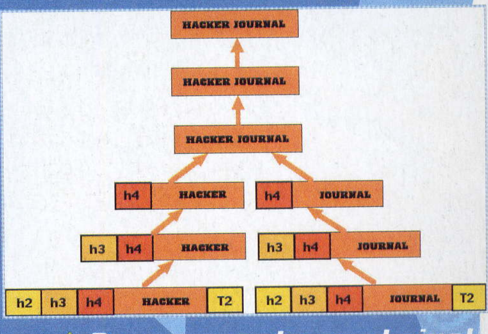
Finalmente hemos recibido el paquete. Se eliminan la primera cabecera y la cola. El paquete está limpio y listo para ser pasado al nivel 3, de Red.



Se comprueba que el paquete sea de verdad para este equipo y se pasa al nivel 4, el nivel de Transporte.



Antes de pasarlo al nivel 5, se descarta la cabecera. Los paquetes que formaban juntos el mensaje completo se preparan para ser reunidos de nuevo.



Recompuesto en el nivel 5, el mensaje se descifra, descomprime, reformatea según se requiera para que recupere el aspecto original. Las cabeceras y colas se han suprimido y la aplicación que lo recibe puede descifrarlo. Tras un largo camino, el mensaje ha llegado, en esta red que utiliza el estándar ISO/OSI.



RSA

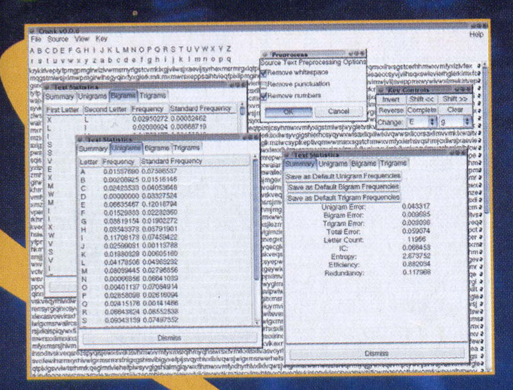
Los desafíos de seguridad son la frontera del criptoanálisis. Hay quien los prueba... y se arriesga a ganar dinero

Los hackers tienen mil intereses. Uno de los más intrigantes es el cracking. Hay cracking bueno y cracking malo; el bueno consiste en hacer saltar sistemas y códigos para demostrar que son débiles, para que se creen otros más fuertes.

En este espíritu se sitúan los desafíos lanzados por los RSA Laboratories: Ampliar la frontera del criptoanálisis, para favorecer la creación de algoritmos mejores y más robustos. Para quien logra violar un desafío hay notables premios en efectivo. ¡Una vez más, quien sea un genio puede ser recompensado adecuadamente!



¡NOS RETA!



¿En busca de instrumentos para el criptoanálisis? ¿Por qué no probar Crank (http://crank.sourceforge.net)?

Factoring Challenge

Números muy grandes: ¿quién logrará factorizarlos, es decir, descubrir qué números primos hay que multiplicar para obtenerlos? Los premios varían de los diez miles dólares para el desafio de 576 bits hasta los doscientos mil dólares para el de 2.048 bits. Todos los detalles están en la página http://www.rsasecurity .com/rsalabs/node.asp?Id=2092.

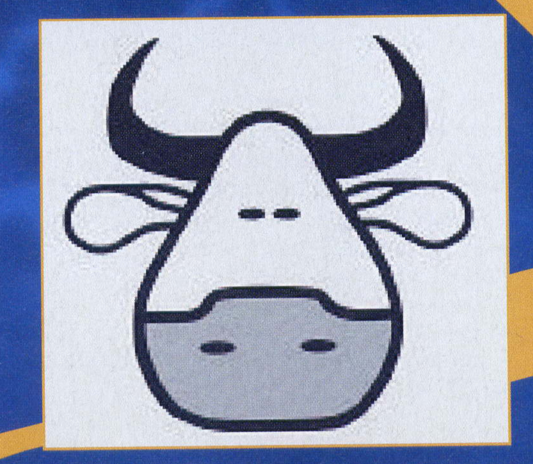
Secret-Key Challenge

Un desafio sobre criptografía DES y doce basados en el cifrado por bloques RC5. La clave de DES es de 56 bits y las doce claves van desde 40 hasta 128 bits. En todos los casos hay de adivinar una frase secreta precedida de tres bloques de texto, conocidos, que contienen la frase The unknown message is: (el mensaje desconocido es:). Todos los detalles están en la página http://www.rsasecurity. com/rsalabs/node.asp?id=2100, incluido el hecho que algunos desafios ya han sido resueltos. Hay todavía ocho activos, cada cual con una recompensa de diez mil dólares.

Para ayudar los potenciales resolvedores también se han propuesto trece pseudodesafíos. Estos no son secretos; el mensaje es conocido. Ni siquiera hay premios, pero permiten verificar el funcionamiento de los propios programas... o adquirir practica sobre las claves RC5.

DES Challenge III

Éste ya ha sido resuelto, en tiempo récord, por la Electronic Frontier Foundation en colaboración con distributed.net. Lo citamos también porque es muy interesante descubrir qué ha sucedido, cómo se ha crackeado el mensaje secreto y otras curiosidades. Los detalles están en la página http://www.rsasecurity.com/rsalabs/node.asp?Id=2108.



Crackers de todo el mundo, uníos

Son desafíos fascinantes, que requieren empeño y estudio y también valen dinero. Es prácticamente imposible conseguirlo solo, pero mediante proyectos como distributed.net, por poner un ejemplo, es posible formar equipos o entrar en teams que tienen probabilidades concretas de conseguirlo y adjudicarse un premio.

¿Quién será el próximo en resolver un desafío? ¿Y si fuera un lector de Hacker Journal? ¡Sería de veras gratificante!

¿QUIÉN HA GANADO?

RSA Security coordina una mailing list dedicada a los anuncios de las soluciones a los retos. La lista tiene poco tráfico y contiene prácticamente sólo anuncios de solución o información importante para los participantes. Para apuntarse basta enviar a majordomo@majordomo .rsasecurity.com un mensaje que contenga en el cuerpo (no en el asunto) el texto subscribe curious-about-secret-key-challenges. Para darse de baja es todo igual, excepto que el texto empieza por unsubscribe.

DNS POISONING Y DOMAIN

¿Hacer creer al mundo que un sitio ha sido atacado desviando las peticiones de los browsers a otro...



Una falsa página Web que responde a la verdadera dirección del sitio. Un usuario ignorante que escriba en la página datos personales... Así funcionan muchas estafas y robos de datos.

Contrainformación, desinformación, terrorismo. Creemos leer una noticia sobre un cierto lugar y en cambio estamos leyendo otra cosa, de otra parte, y alguien ha desviado el camino de nuestro browser sin que éste se haya dado cuenta. Las tácticas para llegar a este resultado son dos: DNS poisoning (o DNS spoofing) y domain hijacking. El primero significa envenenamiento del DNS y consiste en convencer a un servidor de nombres de que un cierto dominio tiene una dirección de IP distinta de la normal. El segundo significa secuestro de DNS y es un verdadero robo de dominio. Ha pasado a la historia la "violación" del sitio de RSA en el 2000. ¡Y RSA se ocupa de la seguridad, pensaron muchos! Pero el sitio no fue violado nunca. Más bien, el falsificador de DNS que lo hizo creó un sitio que parecía el de RSA y luego introdujo información alterada en el servidor de nombres ("envenenando" la caché de éste último: de aquí el vocablo poisoning, de modo que el URL del sitio RSA apuntara, erróneamente, a la página falsa. Cuando el visitante veía la home page falsa alterada, suponía que había sido violado el sitio. La mayor parte de los sitios en el Web son vulnerables a un ataque de este tipo, que es bastante simple y no afecta al servidor Web del sitio, que puede ser protegido cuanto se quiera. No importa; el ataque ni se le acerca.

La clave del spoofing

Cuando escribimos http://www.hacker-journal.com, en realidad escribimos, sin saberto, una dirección de cuatro números. Recordar la dirección numérica es un problema, por lo que se ideó un sistema que traduce de nombre "humano" a número sin que tengamos que hacer nada. Claramente, si alguien cambia la lista de traducciones, la lía.



...sitio, que parece el original atacado? Es posible. He aquí cómo

HIJACKING

Apreciado usuario, estamos instalando un software más seguro. ¿Te importaría volver a insertar tus datos... de modo que esta página falsa de PayPal consiga la información de tu tarjeta de crédito?

El ataque típico en esta situación consiste en alterar el registro del dominio, conservado en Network Solutions para los sitios .com, y otros varios registradores. En la dirección http://www.securiteam.com/securitynews/Domain_Hijacking__A_step-by-step_guide.html se encuentra una guía detallada sobre cómo hacer un ataque a un sitio de ejemplo.

Cómo protegerse

Para prevenir este tipo de ataque es necesario que la seguridad esté en el sistema de gestión de DNS. Si por ejemplo un gestor de dominios acepta por email el cambio de información en el dominio, el mail tiene que viajar cifrado y autenticado mediante PGP, o bien tiene que disponer de una página Web segura para efectuar los cambios. Una de las mejores soluciones aparecidas hasta ahora es DNSSEC, o DNS Security. Este sistema combina criptografía de clave pública con firma digital para autenticar a quien pida información sobre un dominio.
Para protegerse valen las recomendaciones habituales. Una contraseña débil protege menos, es mejor una contraseña robusta; controlar regularmente con WHOIS que los datos relativos a los propios dominios son correctos; mirar las estadísticas de acceso y ver a si hay algo extraño, por ejemplo una caída de visitas repentina y sin razón. Un DNS poisoning no causa daños verdaderos y por ello, si no se está atento, el riesgo es que ni nos demos cuenta. Mientras tanto la gente va a otra página...

LOS CONSEJOS DE NEO

COMPRENDER Y PROFUNDIZAR

DNS: Domain Name System, sistema de nombres de dominio. Los nombres de los dominios existen en forma numérica (como 17.112.152.32: ¿a quién corresponde?), pero para facilitar las cosas se creó un mecanismo que lo traduce en nombres comunes (como www.linux.org: ¿cuál es su forma numérica?). La correspondencia entre nombres y números figura en bases de datos que posee quien vende dominios y luego en una serie de servidores distribuidos por Internet. Cuando el browser pide un sitio, se reenvía a un servidor que da el DNS correcto. Los servidores (DNS server) se actualizan periódicamente con los cambios de información. Si los datos están equivocados, al nombre correcto le corresponde un número equivocado. Network Solutions: http://www.netsol.com. El más antiguo y conocido gestor de nombres de dominio americanos e internacionales.